STANDARD 218-10

TELECOMMUNICATIONS AND TIMING GROUP

TELEMETRY TRANSMISSION OVER INTERNET PROTOCOL (TMoIP) STANDARD

WHITE SANDS MISSILE RANGE
REAGAN TEST SITE
YUMA PROVING GROUND
DUGWAY PROVING GROUND
ABERDEEN TEST CENTER
ELECTRONIC PROVING GROUND
HIGH ENERGY LASER SYSTEMS TEST FACILITY

NAVAL AIR WARFARE CENTER WEAPONS DIVISION, PT. MUGU
NAVAL AIR WARFARE CENTER WEAPONS DIVISION, CHINA LAKE
NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION, PATUXENT RIVER
NAVAL UNDERSEA WARFARE CENTER DIVISION, NEWPORT
PACIFIC MISSILE RANGE FACILITY
NAVAL UNDERSEA WARFARE CENTER DIVISION, KEYPORT

30TH SPACE WING
45TH SPACE WING
AIR FORCE FLIGHT TEST CENTER
AIR ARMAMENT CENTER
ARNOLD ENGINEERING DEVELOPMENT CENTER
BARRY M. GOLDWATER RANGE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

This page intentionally left blank.

DOCUMENT 218-10

TELEMETRY TRANSMISSION OVER INTERNET PROTOCOL (TMoIP) STANDARD

OCTOBER 2010

Prepared by

TELECOMMUNICATIONS AND TIMING GROUP

Published by

Secretariat
Range Commanders Council
U.S. Army White Sands Missile Range,
New Mexico 88002-5110

This page intentionally left blank.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

The Telecommunications and Timing Group (TTG) of the Range Commanders Council (RCC) prepared this Standard. This Standard replaces RCC Standard 218-07, Telemetry Transmission over Internet Protocol (TMoIP) Standard. This Standard provides the ranges with a standards-based solution for the ground transport of serial streaming telemetry from multiple vendors and an improvement in cost competitiveness.

A new chapter (Chapter 4) contains recommendations for implementing the Ground Network. Two new appendixes have been added to provide more information for TMoIP implementation. Appendix F provides additional insight into the management aspects of TMoIP. Appendix G, while not in the scope of the TMoIP requirements, provides information to the user to enable the deployment of a network infrastructure that supports the TMoIP implementation.

Any range that uses telemetry will benefit from this Standard. The purpose of the TTG effort is the identification of the needs of the Major Range and Test Facility Base (MRTFB) community for telemetry (TM) transmission, the identification of commercially available Asynchronous Transfer Mode (ATM) solutions, and development of a standard to ensure future interoperability of commercial solutions. This document presents a common standard for use by industry to ensure interoperability and competition for a more cost effective solution for the ranges. Use of this document will also eliminate the need to rely on a single source for critical equipment in the support of range missions within the MRTFB.

The RCC gives special acknowledgement for production of this document to:

Task Lead: Mr. Dave Bryant
Chair, Communication and Data Transmission Committee
Member, Telecommunications and Timing Group (TTG)
45th Space Wing (45 SW)
Lockheed Martin
P.O. BOX 254307
Patrick Air Force Base (AFB), FL 32925

Phone:	DSN 854-7169	COM (321) 494-7169
Fax:	DSN 854-1519	COM (321) 494-1519
E-mail:	dave.bryant@itt.com	

Please direct any questions to:

Secretariat, Range Commanders Council
ATTN: CSTE-DTC-WS-RCC
100 Headquarters Avenue
White Sands Missile Range, New Mexico 88002-5110
Phone: DSN 258-1107 COM (505) 678-1107,
E-mail wsmrrcc@conus.army.mil

This page intentionally left blank.

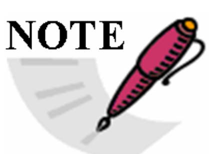
CHAPTER 1

INTRODUCTION AND OVERVIEW OF THE TELEMETRY TRANSMISSION OVER INTERNET PROTOCOL (TMoIP)

This document provides specifications and guidance for the ground network segments, which includes the telemetry (TM) Terminal, Network Processor, and the Ground Network subsystems of a TM range network. This document is for use by equipment vendors in designing products that enable the transport of TM data over IP networks. The "TMoIP solution", discussed in Chapter 2, addresses the Ground Network elements listed below. The Ground Network functional blocks are shown in Figure 2-2. Each of these elements is discussed in detail in subsequent chapters. The requirements and recommendations for the TM Terminal and Network Processor elements are located in Chapter 3. In addition, Chapter 4 addresses the Ground Network implementation via a set of recommendations regarding implementation elements that will enhance the robustness of the TMoIP solution.

a. TM Terminal. The TM Terminal interface provides connectivity to the TM stream. The TM stream interface is described by a set of electrical characteristics, such as waveform amplitude and frequency, and mechanical characteristics such as connector type. This document defines the range of TM stream types to be supported, including the characteristics associated with Layer 1 (Physical Layer) of the Open Standard Interconnect (OSI) Model (see paragraph 3.3).

b. Network Processor. The Network Processor furnishes the bulk of the TMoIP solution, and consists of the TM stream interface, the TM stream processing, and the Ground Network interface. The scope of this document is to define the requirements for the Network Processor associated with OSI Layer 7 through OSI Layer 1.



While this document refers to TMoIP, the requirements for the Network Processor at Open Standard Interconnect (OSI) Layer 1 and OSI Layer 2 are also within the scope of the TMoIP implementation.

c. Ground Network Link. This link provides IP network connectivity and transport of the TMoIP traffic. The Ground Network includes the network end equipment, typically an IP switch or router, and the interconnecting network. In some cases, the interconnecting network may not be an IP network, but may be a Synchronous Optical Networking (SONET) or Asynchronous Transfer Mode (ATM) implementation. In these cases, the network end equipment may include functionality to perform the required adaptation from the IP switch/router to the native network format.

This page intentionally left blank.

CHAPTER 2

TELEMETRY (TM) TRANSPORT TECHNIQUES

This chapter provides an overview description of TM systems. Included are the major functions of a TM system and current methods for distribution of TM streams via range communications infrastructures. Additionally, the motivations and technical challenges for implementing TM stream transport over IP networks are presented. Subsequent chapters address the detailed specifications that define the TMoIP implementation.

2.1 Telemetry (TM) System Overview

Telemetry (TM) is the method of getting data from vehicles during operational launches, test missions, and a variety of other applications (see RCC Document 106-07 Part I - *Telemetry Standards* (Reference a), and RCC Document 106-07 Part II - *Telemetry Networks* (Reference b). In this section, the different segments that constitute a TM system are discussed. The segments of a generic TM system are shown in Figure 2-1.

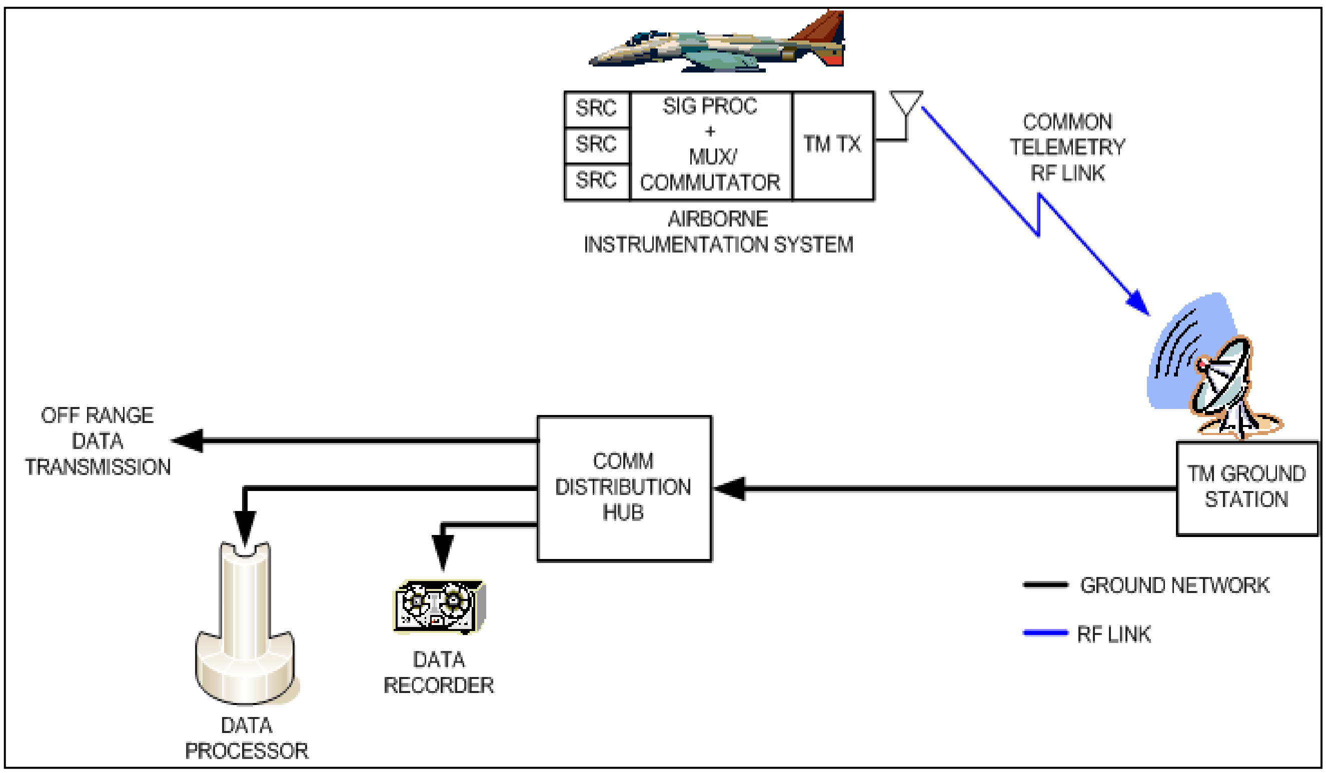


Figure 2-1. Generic TM system.

The segments of a TM system are:

a. Airborne Instrumentation System (AIS).
b. Common telemetry radio frequency (RF) link.
c. TM ground station.
d. Ground Network.
   (1) Communications Distribution Hub (CDH).
   (2) Data processor.
   (3) Off range data transmission.
   (4) Data recorder.

The overall TM goal is to get information that characterizes the operation of the vehicle to the engineers and end users who need it. If any one of the above segments does not function correctly, the data will not be available when needed.

2.1.1 Airborne Instrumentation System (AIS). The AIS consists of the TM source (SRC), the Signal Processing and Multiplexer/Commutator function (SIG PROC + MUX/COMMUTATOR) and the TM Transmitter (TM TX).

a. Telemetry Source (SRC). The TM SRC originates as an output of a transducer or other information source that represents a quantity (such as temperature or mechanical strain) to be measured or monitored.

b. Signal Processor (SIG PROC). The SIG PROC controls the relevant characteristics of the TM source (such as amplitude, offset, and frequency) to allow interface compatibility with downstream circuitry, and to enhance signal integrity and quality.

c. Multiplexer/Commutator (Mux/Commutator). The MUX/COMMUTATOR function allows multiple TM sources to be combined for transmission. The output is the combined information generated by one or more individual information source(s) that have been appropriately processed for optimal fidelity. The resulting composite TM source signal is fed to the TM transmitter for transmission as an RF signal to the TM Ground Station.

d. Telemetry Transmitter (TM-TX). The TM-TX provides the functions required for RF transmission and includes components such as the RF modulator, amplifier, and antenna. The output of the TM-TX is an RF signal that conveys the composite TM source information to the ground for reception, demodulation, and transport to the required end points.

2.1.2 Common Telemetry RF Link. The Common Telemetry RF Link provides the connectivity from the AIS to the TM Ground Station.

2.1.3 TM Ground Station. The functional blocks at the TM Ground Station include receiving antenna(s), TM receiver(s), and demodulator(s) as required to regenerate the source TM streams. The source TM streams, once they have been recovered from the RF Link, are available for transport to the various end stations as required over the Ground Network.

2.1.4 Ground Network. The Ground Network provides distribution of the TM streams from the TM Ground Station to destinations that require the TM stream for analysis, storage, and monitoring.

a. Communications Distribution Hub (CDH). The TM Ground Station is connected to the CDH. The function of the CDH is to forward the TM streams to the required end stations. The end stations can provide recording capability (Data Recorder), analysis, and post-processing (Data Processor), or transmission to off-range locations (Off Range Data Transmission).

b. Data Processor. The Data Processor supports processing of the telemetry data and includes functions such as bit or frame synchronization, decryption/encryption, error correction algorithms, coding, and timing functions along with data reduction algorithms.

c. Data Recorder. The Data Recorder provides the capability to record telemetry data in support of store and forward or playback mission requirements.

d. Off Range Data Transmission. The Off Range Data Transmission facility allows the telemetry data to be transported to remote locations for monitoring or additional processing.

The number of destination points that exist on the Ground Network, and the potential requirement to forward the TM stream simultaneously to more than one destination point, reveals the requirement to support multicast transmission of the TM streams over the Ground Network. The ability to natively support multicast traffic is one feature that makes IP transport of TM streams very desirable.

2.1.5 Telemetry Over IP (TMoIP). The TMoIP involves the transport of the telemetry streams in the Ground Network over a packet switched network. Examples include telemetry stream transport from the TM Ground Station to Off Range Transmission, Communications Distribution Hub to Data Recorder, etc. Use of the IP protocol as the packet network of choice facilitates using commercial switches and routers that are based on the IP protocol in the Ground Network.

A model for the transport of TMoIP in the Ground Network is shown in Figure 2-2.

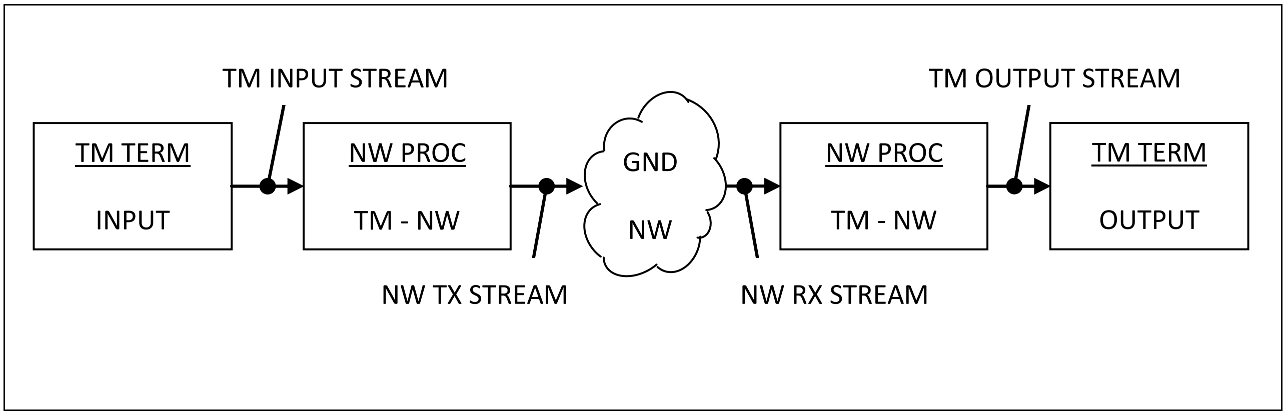


Figure 2-2. Ground Network functional blocks.

There are three basic functional blocks associated with the Ground Network that participate in TM stream transport: the TM Terminal, the Network Processor, and the Ground Network Link.

a. TM Terminal (TM TERM). The TM TERM functional block provides connectivity to the native TM stream. At the Ground Network ingress, the TM Terminal block provides the TM Input Stream to the Network Processor. At the Ground Network egress, the Network Processor receives the Network RX stream, generates the TM Output stream, and sends it to the TM Terminal.

b. Network Processor (NW PROC). The Network Processor provides the TMoIP functions to the Ground Network.

   At the ingress to the Ground Network, the Network Processor receives the TM Input Stream and provides the required TMoIP formatting and adaptation to enable transport over the Ground Network. The end product of the Network Processor is the Network Transmit (NW TX) Stream.

   At the Ground Network egress, the Network Processor receives the TMoIP Network Receive (NW RX) Stream and performs the inverse formatting process to recover the TM stream. An additional important function of the Network Processor at the Ground Network Egress is to recover the TM clock information such that the TM Output Stream has timing characteristics identical to the TM Input Stream.

c. Ground Network Link (GND NW LINK). The Ground Network Link provides the actual transport that carries the Network Stream between locations over a packet switched network.

   The goal of the Network Processor and Ground Network is to provide seamless transport for the TM stream. Ideally, the TM Input Stream should be identical to the TM Output stream except for the delay introduced by the transport process.

The following sections describe a number of implementations for Ground Network transport of native TM streams. This subsystem has evolved from dedicated point-to-point (fiber or microwave), proprietary solutions requiring a dedicated DS3 link (45 Mbps), to ATM based solutions, and finally to the IP-based solutions that are currently emerging.

(1) Time Division Multiplexing (TDM). The TDM transport formats the TM traffic as a single (or group) of bit streams. TDM typically supports a number of simultaneous transmission channels, where the transmission link is divided into a fixed number of channels, and each channel has a constant bandwidth. The timeslot for each individual channel is recurring and pre-allocated to that channel. Although TDM provides basic transport capability, current implementations are proprietary and do not lend themselves to multicast support. Further, the fixed bandwidth of TDM connections can result in inefficient bandwidth usage and stranded bandwidth if the traffic does not conform to the TDM link capacity.

(2) Asynchronous Transfer Mode (ATM). ATM is a protocol in which data traffic is formatted into fixed length (48 data bytes + 5 bytes of header) packets for transmission through the network. ATM is a connection-oriented technology, where a connection must be established between two endpoints before actual data transfer can begin. Support for multicast traffic is not an inherent part of the ATM protocol, and is dependent upon vendor implementation. The ATM protocol lends itself well to the transport of TM streams due to the following properties:

- Through the Circuit Emulation mechanism, ATM supports transport of TDM streams.
- The small fixed packet size produces minimal cell jitter.
- ATM supports built-in Quality of Service (QoS) mechanisms to ensure timely packet delivery.

Additionally, ATM is well suited for use with Plesiochronous Digital Hierarchy (PDH) DS3 or Synchronous Optical Networking (SONET) Optical Carrier 3 (OC3), Optical Carrier 12 (OC12), etc., physical network configurations, and provides a straightforward migration for use in many existing range networks.

Although ATM supports packet switching and QoS mechanism that ensure packet delivery, but it is a connection-oriented protocol, requiring connections to be configured prior to transmission.

(3) Internet Protocol (IP). This protocol is one where data traffic is formatted into variable-length packets, referred to as datagrams; however, in contrast to the ATM protocol, the packet size can vary from 64 to 1536 bytes.

NOTE	The IP documents use the term datagrams for the unit of exchange. In an effort to remain consistent with existing proposals for the transport of serial streams over IP networks (Pseudo Wire) and for the transport of TM streams over IP networks (Packet TM), the term packet will be used in this document to refer to the unit of exchange of TM traffic over IP networks.

NOTE	The IP is a “connectionless” protocol, whereas ATM protocol is not. Connectionless means that a connection does not need to be made before a host can begin transmission to another host with which it has not previously communicated.

TM streams place strict requirements on delivery because they are real-time traffic streams; if a packet does not arrive to its endpoint in a known and dependable fashion, the data is lost. The support of the transport of real-time streams such as TM traffic over IP networks requires QoS mechanisms for IP networks, and the support for these mechanisms in the end equipment. Recent developments in protocol extensions to IP to support QoS have produced a number of QoS mechanisms to support reliable delivery of TM traffic.

2.2 Motivation for Telemetry Transmission over Internet Protocol (TMoIP)

There are number of reasons and motivations for providing the capability to transport TM streams over IP networks. IP technology is emerging as the packet technology of choice for a variety of networking uses, ranging from traditional data applications to real-time applications such as voice and video transport. With the maturation of the technologies that have enabled the transport of voice and video streams over IP networks, this same technology is envisioned to be applied to the transport of TM streams over IP networks.

Due to the proliferation of IP networking products (and the associated economies of scale for technical and manufacturing), performance has increased while equipment costs have decreased. Therefore, implementations of IP benefit from increased capabilities and lower costs.

Another benefit of TMoIP comes in the form of operational support. Since IP is very widespread, the skill set of the operators becomes less specialized to support one more capability over the ubiquitous IP network. An IP technology technician can be cross-trained on TM (as a new service) and support the TM mission in a relatively short amount of time. This approach addresses perhaps the single biggest issue facing range managers today: the turnover of qualified people supporting the mission.

In terms of mission management, transport technology has evolved from TDM solutions to ATM solutions. Although ATM has generated cost savings and also increased capability, ATM methods are perceived as complex. One reason for this is that ATM is a connection-oriented technology that requires that ATM connections be provisioned for each TM stream. In contrast, IP is a connectionless technology, meaning that no equipment configuration is required prior to transmission. Coupling the connectionless nature of IP with improved management tools that will become available as the commercial world advances will enable solutions like TMoIP to simplify the operational requirements of the networks and make them easier to deploy.

Applying the IP capability in the range and TM world is fairly uncomplicated. The support requirement is to link the receiving station to the end terminating station over a packet network. The operators still have the task to identify which resources to link together, but today this becomes an exercise in network management, for which there are network management tools becoming available should making the effort straightforward.

Another motivation for migration to TMoIP is the native support of multicast traffic provided by the IP protocol. Multicast techniques support reception by multiple users without replicating the traffic to each user. Additionally, by using multicast techniques, a bandwidth-efficient scheme can be implemented to perform TMoIP transport. This scheme works as follows:

a. The NW TX Stream is constructed to be a multicast IP stream. This construction essentially results in the generation of an IP stream with an address in a specific range, indicating that it is a multicast stream.
b. The TM Terminals needing to receive the multicast stream notify their local IP switch or router that they want to receive the stream; notification is made using an IP protocol called Internet Group Management Protocol (IGMP). The IGMP provides support mechanisms to support efficient transport of multicast traffic in IP networks (see Chapter 4).
c. When a switch or router receives a request from a TM Terminal, it will forward the Network RX Packets that carry the TM stream to the TM Terminal.

   If a switch or router receives a multicast packet and there are no local or downstream TM Terminals that want to receive it, the packet will not be forwarded. In this fashion, network bandwidth is only consumed when a TM Terminal requires it; therefore, the need to build connections for every link is eliminated and the configuration is simplified.

2.3 Challenges for TMoIP

A number of technical requirements and challenges must be addressed in the TMoIP implementation before the advantages of IP network integration can be obtained.

2.3.1 Downlink Data Requirements. Downlink data may originate from a variety of sources such as a launch vehicle, payload, aircraft, ship, and/or weapon platform. Downlink data requirements are fairly common across Department of Defense (DoD) Services because the mission requirements have typically data sent in a serial stream; additionally, the timing source normally uses an on-board oscillator.

Downlink data is handled in several ways. Many operations require the recording of data at the first receiving site to preserve the data and to ensure all data is available. Other operations record at the data processing equipment location. Many missions support on-board recording for post-flight and only use the ground based recording in case the on-board copy is corrupted.

During a real-time test, there is typically no time or available bandwidth for re-transmission of errors.

Difficulties arise when transmitting downlink data across a network having different timing characteristics than those of the source TM stream. This problem has been the challenge with TM since the beginning of real-time mission support. The isochronous nature of the TM stream using the on-board oscillator can be exacerbated by a number of causes that can affect timing, including Doppler and multi-path effects. Given the critical nature of the timing information contained in the source TM stream, it is important that the TMoIP solution address the requirement to accurately and reliably transport and regenerate the source TM timing across the network.

The requirement for delay is very subjective. Most users will say “as fast as possible” without being able to quantify. Typically, the most stringent requirement on delay is either voice or range safety. Typical range safety requirements state that from an event on the vehicle to the time the Flight Termination System (FTS) signal is received at the vehicle shall not exceed one second, not counting three seconds allotted for human processing. This requirement often translates into a requirements allocation of 100 milliseconds for the transmission of data from the receiving station to the data processing building. In the case of voice, audio embedded in the TM stream is often used to communicate with the test personnel as a hot-microphone. If the TM transmission is delayed, an uncomfortable pause is noticed in the conversation and an echo is added that must be removed when the Ultra High Frequency (UHF)/Very High Frequency (VHF) radio is used on the ground. Because echo cancellers can be used for the delay, the uncomfortable pause is the driving factor for a delay requirement that does not exceed 100 msec. Traditionally, the delay introduced by the transport process was mainly caused by stream processing and end-to-end transit time. As the IP protocol is packet-based, the conversion of the source TM streams to packets introduces an additional delay component that must be included in the total system delay. This packetization delay can be a significant component of the total system delay, especially at low TM rates.

Path-delay control mechanisms provide alignment of TM streams in the following scenarios:

a. A single TM stream enters the network at different points and is received at a single site. Due to the differential path delays, the multiple receive-streams must be re-aligned.
b. A number of TM streams enter the network at different points and are received at a single site. Again, due to the different path delays, these streams must be aligned so that the data corresponds in time.
c. A number of TM streams of diverse rates enter the network and are received at a single site. Due to the differential delays introduced by packetizing each stream, the streams must be aligned to enable the data points to correspond in time.

Potentially the biggest issue with providing a successful TMoIP solution is that IP is a best effort service without guaranteed service delivery. The lack of guaranteed delivery of TM packets can result in negative effects such as packet jitter, network congestion causing out-of-order packets and potential packet loss, affecting clock regeneration and recovery. To enhance the network QoS for TMoIP, QoS mechanisms available in Commercial off the Shelf (COTS) network equipment are used. Providing guidance for the provision of effective QoS is an important part of the TMoIP solution. The subject of QoS support is addressed in detail in detail in Chapter 4.

2.3.2 Uplink Command Requirements. Uplink commands are different from downlink commands because the data rate is typically much lower and the entire message must be received without a single bit error. The uplink data used for platform or payload reconfiguration is, in many cases, a pre-determined event that can be pre-loaded from the mission control computers to the RF uplink station. Therefore, the transport mechanism for uplink streams must support message validation and re-transmission. The implementation for message validation is reserved for the application layer.

2.3.3 System Management. Systems management in today’s environment means selection of one of a number of options, including manual patch panels, DS3 cross-connect, and ATM connections. The use of TMoIP provides opportunities to simplify the provisioning control plane of the network by self-routing protocols available in every IP network today.

Local management operations provide the mechanism to provision and manage local end equipment. To support management operations for equipment located at distant locations, remote management methods are employed. In-band or out-of-band and management methods can be used with TMoIP to support provisioning, statistics, and fault management. Protocols such as Hypertext Transfer Protocol (HTTP) and Simple Network Management Protocol (SNMP) are available to provide the remote management capability.

This page intentionally left blank.

CHAPTER 3

TMoIP PAYLOAD CONSTRUCTION

3.1 Overview/Management Elements

In the preceding chapters, existing TM transport techniques and challenges for migration to using Internet Protocol (IP) networks as a transport medium were discussed. In this and following chapters, the requirements for the implementation of a TMoIP solution are developed.

Chapter 3 describes the TMoIP payload details. Chapter 4 defines management elements to enable status reporting, configuration, and integration with the end equipment that, with the TM Terminal, comprises the Ground Network.

3.1.1 TMoIP payload. A payload structure is defined that provides sufficient flexibility to allow the user to optimize for payload efficiency and different network topologies, yet provide inter-working capability between different vendors.

3.1.2 TMoIP solution. The TMoIP solution includes management activities such as:

a. Addressing the requirement to accurately and reliably regenerate the source TM timing at the network receiver by including objective specifications for the performance of the clock regeneration function.
b. Recommending mechanisms to control path delay, as well as the capability to provide the alignment of TM streams.
c. Identifying a number of methods by which network equipment provides support for Quality of Service (QoS), and provide support for these methods, while allowing the user to provision the optimal QoS solution.
d. Including provisions for maintenance and management support. Both in-band and out of band methods will be defined. In-band methods support the requirement for status information to be transported concurrently with the TM traffic, and out-of-band methods provide the capability to provide extended management features.

In addition to the above management elements, Chapter 4 will address TMoIP implementation issues relating to network performance, reliability, and multicast traffic considerations.

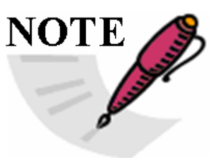
3.2 High Level Requirements (Concept of Operations)

For full understanding of the TMoIP requirements, the user is directed to the major user operational requirements shown below in Table 3-1. These high-level requirements drive each of the detailed specification requirements discussed later in this document. The TMoIP solution must meet the requirements shown in Table 3-1.

TABLE 3-1. HIGH LEVEL REQUIREMENTS

Req/Opt[(1)]	Requirement description
Req	Accurately and reliably transport and regenerate the source TM data and timing across the network.
Req	Support an Encode/Decode latency of less than 100 milliseconds for the TM input stream to the TM output stream for the following TM rates: 100 Kb/s < TM Stream Rate < 35 Mbps
Req	Enable the use of Quality of Service (QoS) mechanisms that are available in Commercial Off the Shelf (COTS) network equipment.
Req	The transport mechanism for uplink streams must support message validation and re-transmission.
Req	Support local and remote management mechanisms to provision and monitor the TMoIP equipment.

[1] Req = Required, Opt = Optional, Note = notes



In this Standard a series of Requirements, Options, and Notes will indicate the elements that make up the TMoIP implementation. Note that "Req" indicates a required element for TMoIP, "Opt" indicates an optional element, and "Note" indicates notes, recommendations, and informational items.

3.3 Open Standard Interconnect (OSI) Layered Approach

The OSI protocols are a family of information exchange standards. The OSI Model describes seven layers of interconnection: the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer.

For purposes of defining the TMoIP payload, this TMoIP interface standard will identify the interface requirements as they relate to the OSI protocol layers for the TM Terminal and Network Processor (NW PROC) functional blocks that were defined within the Ground Network at Figure 2-2.

In Figure 3-1, the OSI layer structure is shown for the TM Terminal and NW Processor functions for the TMoIP data plane. A red line traces the path of a source TM stream (TM Input Stream) from Layer 1 of the TM Terminal to the Network Processor where ultimately the Network TX Stream is produced for transport via the IP network. Conversely, the green line is the path of the IP traffic (NW RX Stream) through the Network Processor to the TM Terminal, where it finally appears as the TM Output Stream.

The TM Terminal implements a single layer (Layer 1) in the OSI Model, with Layer 2 through Layer 7 being null layers. The Network Processor implements Layer 6 and Layer 4 through Layer 1 of the OSI Model, with Layer 5 and Layer 7 being null layers.

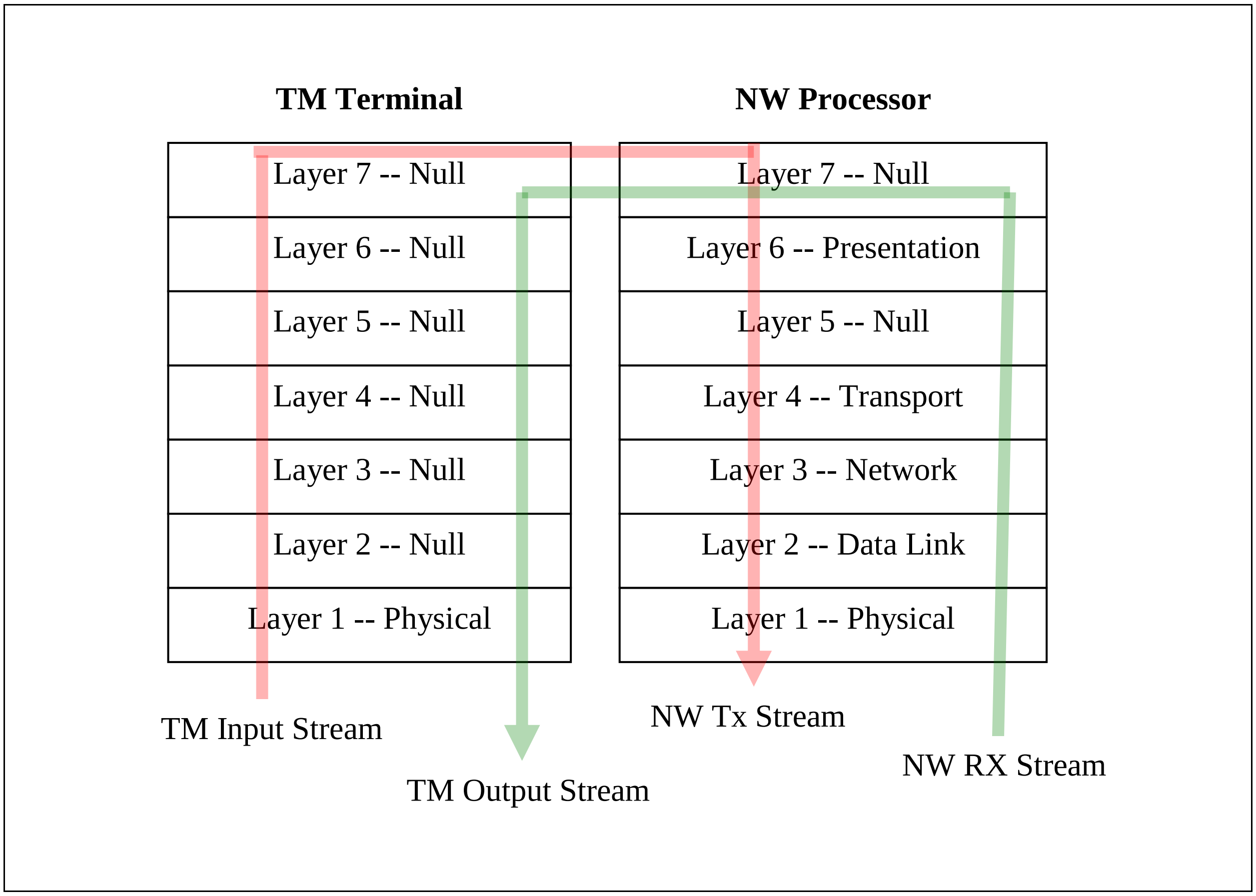


Figure 3-1. OSI Layers for TM Terminal and NW Processor.

NOTE	Throughout this standard, references are made to the International Institute of Electrical and Electronics Engineers (IEEE) Standard 802. The 802 series is a family of IEEE networks standards.

Table 3-2 gives a brief description of each OSI protocol layer and the specific requirements for the TMoIP implementation as each relates to each of the OSI layers.

TABLE 3-2. TMoIP OPEN STANDARD INTERCONNECT (OSI) PROTOCOL LAYER IMPLEMENTATION

Layer ID and Description	TM Terminal	NW Processor
Layer 7 - Application Provide user interface to network	Null layer	Null layer
Layer 6 - Presentation Data transformation such as encoding and encryption to provide standard application layer interface	Null layer	Stream to packet convergence
Layer 5 - Session Establish, manage and terminate connections	Null layer	Null layer
Layer 4 - Transport Provide link reliability, flow control, and error control	Null layer	UDP TCP
Layer 3 - Network Data transport at network level, functions include routing	Null layer	IP IGMP
Layer 2 - Data Link Data transfer between network entities, detect and correct errors in Physical layer	Null layer	802.3 802.1.p 802.1Q
Layer 1 - Physical Defines physical interconnections and the electrical specification of the signals	TM stream physical interface TM stream electrical interface TM stream coding	10BASE-T, per 802.3i 10BASE-F, per 802.3j 100BASE-TX, per 802.3u 100BASE-FX, per 802.3u 1000BASE-X, per 802.3z 1000BASE-T, per 802.3ab

3.4 OSI Protocol Layer Implementation: TM Terminal

3.4.1 Layer 1. Layer 1, the Physical layer, provides the electrical and mechanical interface for the TM Input Stream and the TM output stream from the TM Terminal to the Network Processor.

The Layer 1 properties include physical, electrical, and signal encoding interface. The range and scope of these properties preclude their inclusion in the body of the TMoIP protocol document. To promote interoperability and to provide a baseline interface definition, a set of recommendations and guidelines is provided in Appendix C.

3.4.2 Layers 2 - 7. The remaining TM Terminal layers are null layers, meaning that no processing is performed and no overhead is added. The Application Layer (Layer 7) will provide connectivity of the TM stream to the OSI protocol stack for the Network Processor.

3.5 OSI Protocol Layer Implementation: Network Processor

3.5.1 Layer 7 - Application. The Application Layer in the Network Processor is a null layer and provides the TM stream interface to the TM Terminal.

3.5.2 Layer 6 - Presentation. Layer 6 of the OSI Model provides data transformation and conversion functionality. In the TMoIP solution, this layer provides the payload convergence function that enables the TM stream to be carried over packet networks.

a. Payload Convergence. The payload convergence function converts the serial TM stream into a format compatible with transport over packet switched networks. As the implementation described is similar to the scheme used in Pseudo Wire emulation techniques for the emulation of serial services over packet switched networks, the nomenclature used in the description of Pseudo Wire implementations will be used (see Reference c, (Pseudo Wire_1), Reference d, (Pseudo Wire_2), and Reference e, (Pseudo Wire_3)).

The Payload convergence sub-layer provides the following functions:

(1) TM stream format conversion from a serial stream into a packet format. The resulting packet will be referred to as the Raw Packet Payload.

(2) Appending of TMoIP Control Word to the Raw Packet Payload.

The resulting structure will be referred to as the TMoIP Payload. A TMoIP Payload has the format shown in Figure 3-2.

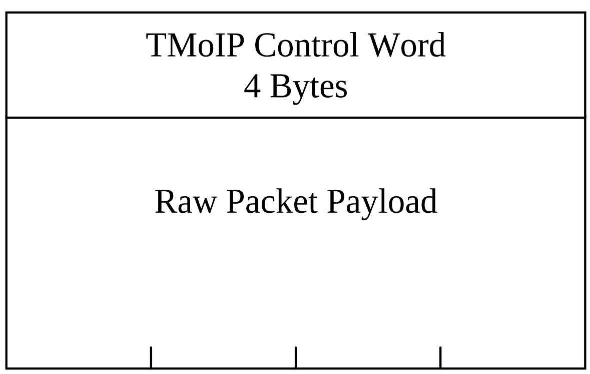


Figure 3-2. TMoIP Layer 6 implementation.

b. TMoIP Control Word Format. The TMoIP Control Word is pre-pended to the raw packet payload and supports the following functions:
(1) Detection of packet loss or packets out of ordering.
(2) Ability to identify failures in local TM interface.
(3) Fault signaling capability across the network.

The format of the TMoIP Control Word is shown in Figure 3-3.

RES	L	R	M	RES	LEN	SEQ NUMBER

Figure 3-3. TMoIP Control Word.

The TMoIP Control Word fields are defined in Table 3-3.

TABLE 3-3. TMoIP CONTROL WORD

Field	Bits	Description
RES	4	Reserved, Code to "0000".
L	1	Local Defect Alarm, indicates local circuit fault in the TM stream
R	1	Remote Defect Alarm, indicates remote circuit fault in the TM stream
M	2	Local Defect Alarm Modifier
RES	2	Reserved
LEN	6	If non-zero, LEN indicates TMoIP Payload Length, defined as the TMoIP Control Word + Raw Packet Payload If zero, LEN indicates TMoIP Payload Length greater than 63 bytes. In this case the TMoIP payload length is determined via length fields in lower protocol layers.
SEQ NUMBER	16	Sequence Number

Notes

Req The TMoIP raw packet size shall be user configurable.
Opt The TMoIP raw payload size may be auto-configurable, based on user priorities (e.g. stream/delay characteristics).
Req The minimum TMoIP raw packet size = 1 byte.

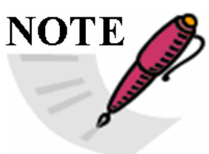
Notes: a. To limit the effects of Ethernet fragmentation, the final Layer 2/3/4/6 packet size should be less than the Ethernet Maximum Transmission Unit (MTU).
b. Padding may be required to meet the minimum Ethernet MTU size.

c. Packet Size. A number of considerations drive the choice of packet size. Table 3-4 illustrates the operational tradeoffs between small packet size and large packet size.

TABLE 3-4. PACKET SIZE TRADEOFFS

Small Packet	**Large Packet**
High Overhead	Low Overhead
Low Latency	High Latency
Low Delay Variation	
High sample resolution for clock recovery	

From Table 3-4, it would appear that small packets have superior operational characteristics as compared to large packets. However, the benefits of lower latency and delay variation advantages are diminished for high bit rate TM streams greater than 1 Mbps. The advantage is reduced because the packetizing latency decreases as the bit rate of the TM stream increases. In such cases, the desirability for the use of large packets, and the reduced overhead that they incur, increases. It is thus concluded that some user control of the packet size be supported to provide the user the ability to optimize system performance.



Support for packet designs that simplify inter-working with alternate protocols may be included. One example is to provide the capability to generate packets that can be efficiently packed into Multi-Protocol-Over-Asynchronous Transfer Mode (Request For Comments (RFC) 2684) cells.

Packet length will be revisited upon definition of the balance of the protocol layers.

d. Timing. In addition to the payload convergence function, the TMoIP implementation must support timing functions that result in the accurate regeneration of the telemetry stream timing characteristics at the receive interface.

In these cases, the receive interface must regenerate the native TM stream as it was inserted to the network at the transmit interface. Therefore, two timing-related design mechanisms to be considered are clock recovery and timed payload delivery.

(1) Clock Recovery. Clock recovery is the extraction of output transmission bit timing information from the delivered packet stream. The TMoIP stream carries the timing information natively, but extracting timing from a highly jittered source requires an algorithm that reproduces the source TM clock with the required accuracy and dynamic characteristics. Two basic mechanisms exist: adaptive clock recovery, and real-time protocols (RTP), such as described in Reference f.

Req	Adaptive clock recovery support is required for TM clock regeneration

The definition for the TMoIP payload that supports RTP is included here. For a TMoIP payload that supports RTP, the payload is formatted as in Figure 3-4.

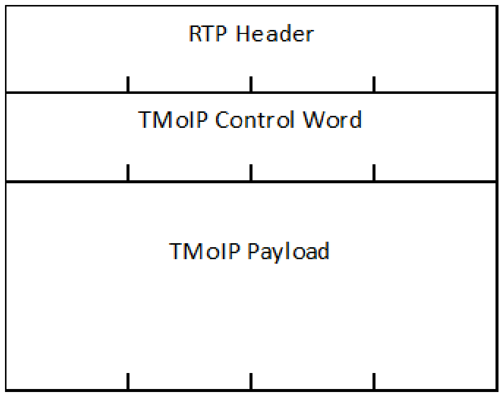


Figure 3-4. TMoIP Layer 6 RTP implementation.

Opt	RTP support is optional.

Req	The clock recovery algorithm must display the following performance characteristics:		
Spec	Min	Max	Notes
Jitter			Per IRIG 106 Chapter 4
Wander			Per IRIG 106 Chapter 4
Acquisition Time		N/A	TM stream rate < 64 Kbps
Acquisition Time		2 sec	TM stream rate > 64 Kbps Acquire to + 500 ppm from stream resynchronization

NOTE	The parameters and requirements for Acquisition Time are items for further study and will be updated in future revisions of this document

(2) Timed Delivery. For the TMoIP function, timed delivery is the ability to control the relative phase (skew) of more than one TM stream at the output interface. This function allows the user to perform temporal alignment of the recovered streams and equalize any delays incurred by packetizing time or network transmission time. Some situations where temporal re-alignment of TM streams is required are:

- A single TM stream enters the network at different points and is received at a single site. Due to the differential path delays, the multiple receive streams must be re-aligned.
- A number of TM streams enter the network at different points and are received at a single site. Again, due to the different path delays, these streams must be aligned so that the data corresponds in time.

- A number of TM streams of diverse rates enter the network and are received at a single site. Due to the differential delays in stream packetization, the streams must be aligned to enable the data points to correspond in time.

Opt	Support for timed delivery is optional at this time, but equipment vendors are urged to consider implementation of this feature in their equipment.

3.5.3 Layer 5. (Null)

3.5.4 Layer 4. Layer 4 defines mechanisms for providing end-to-end communication control in order to ensure reliable transport of data across the network.

a. User Datagram Protocol (UDP). In the TMoIP implementation, the UDP (see Reference g) provides a datagram mode of transport of TM streams over a packet-switched network. This protocol assumes that IP is used as the underlying protocol. The UDP header is appended to the TMoIP Layer 6 Payload, and consists of eight bytes. The TMoIP packet with the UDP header added is shown in Figure 3-5. The un-shaded block is the overhead added by the UDP header.

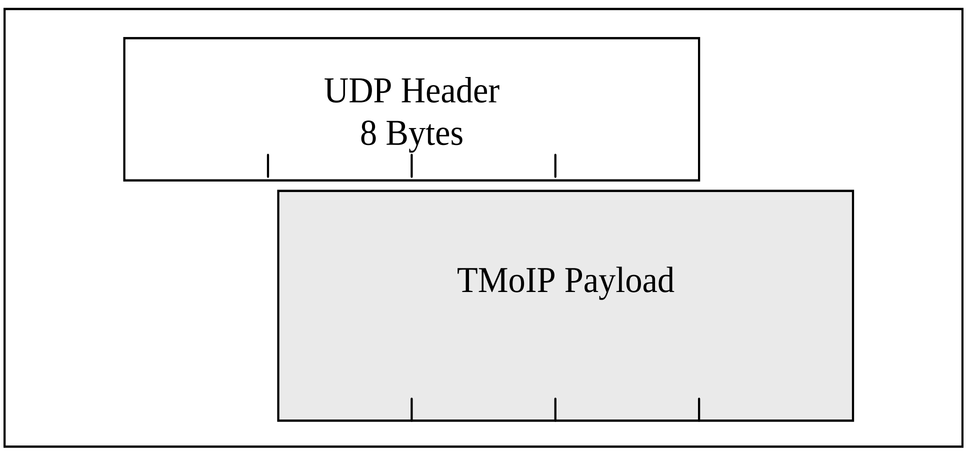


Figure 3-5. TMoIP Layer 4 - Layer 6 implementation.

The UDP header fields are described in Table 3-5.

TABLE 3-5. USER DATAGRAM PROTOCOL (UDP) HEADER FIELD DESCRIPTIONS

Field	Len	Description
Source Port	2	Port number of sending process
Destination Port	2	Port number of receiving process
UDP Length	2	Length of UDP datagram
UDP Checksum	2	Checksum of UDP header + data

The UDP Header field requirements for TMoIP are described in Table 3-6.

TABLE 3-6. UDP HEADER FIELD REQUIREMENTS

Field	Notes
Source Port	Provide ability for user to modify
Destination Port	Provide ability for user to modify
UDP Length	Calculated value
UDP Checksum	Calculated value

The UDP protocol provides the following functions:

(1) Check-summing of the packet for error detection.
(2) Support for stream multiplexing. The UDP port is used to support the multiplexing of traffic to a host. In the TMoIP implementation, the UDP port can be used to multiplex the following stream types:
- individual TM Input/TM Output streams, which can be multiplexed by assigning a different UDP port to each stream.
- Management streams, which can be differentiated from TM stream traffic by assigning them to a specific UDP port. UDP port numbers are managed by the IANA. The port numbers are divided into three ranges named the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports, described as follows.
    - The Well Known Ports are those from 0 through 1023. These ports should not be used without Internet Assigned Numbers Authority (IANA) registration.
    - The Registered Ports are those from 1024 through 49151. These ports should not be used without IANA registration.
    - The Dynamic and/or Private Ports are those from 49152 through 65535, and are available for use by private individuals.

Req	UDP protocol support shall be included in the TMoIP implementation

Opt	The TMoIP implementation may provide the capability to assign a separate UDP port to each TM stream

Opt	The TMoIP implementation may provide the capability to assign a separate UDP port to management streams

Req	The TMoIP implementation shall support the use of UDP ports 49152 through 65535

b. Transmission Control Protocol (TCP). An alternate Layer 4 protocol is TCP, (Reference h). In contrast to UDP, TCP provides reliable end-to-end packet delivery using a structured send/receive protocol that includes the acknowledgement of data packets. If a lost packet is detected during transmission, the packet is re-transmitted. While this mechanism works well for the delivery of data traffic without strict timing requirements, it does not lend itself well to the transmission of real-time traffic, because the time it takes for packet retransmission exceeds the delivery requirements for most real-time streams. Additionally, TCP is a point-to-point protocol and does not support multicast traffic.

NOTE	TCP implementations may be considered in future versions of the TMoIP standard.

3.5.5 Layer 3. Layer 3 of the OSI Model provides routing functionality across a sub-network. TMoIP will use the IP protocol as the layer 3 mechanism (Reference i, IPv4).

The IP header is appended to the TMoIP Layer 4/Layer 6 Payload, and consists of 20 bytes. The TMoIP packet with the IP header added is shown in Figure 3-6. The un-shaded block is the overhead added by the IP protocol layer.

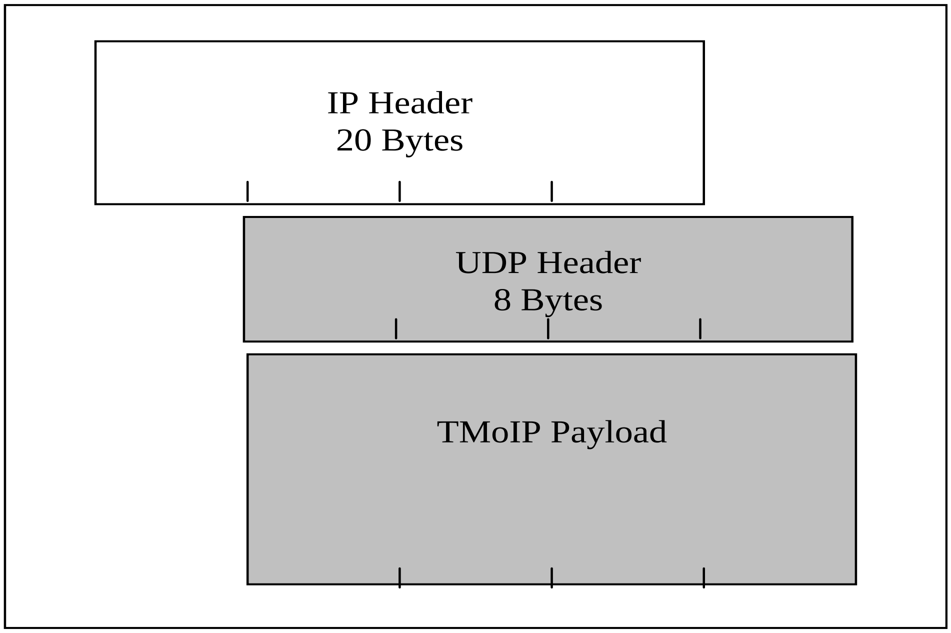


Figure 3-6. TMoIP Layer 3 - Layer 6 Implementation.

The IP header fields are described in Table 3-7.

TABLE 3-7. IP HEADER FIELD DESCRIPTIONS

Field	Length	Description
Version Header Length	1	Bits 0 – 3 = Version Bits 4 – 7 = IP header length
Type of Service	1	TOS, set QoS for particular type of traffic
Total Length	2	Total length of IP packet
ID	2	16 bit ID
Flags Fragment Offset	2	Bits 0 – 3 = flags Bits 4 – 15 = Fragment Offset
Time to Live	1	TTL, number of hops that a packet can travel before being discarded by a router
Protocol Type	1	Protocol, as defined by IANA registry
Header Checksum	2	IP Header CRC
Source Address	4	Source IP Address
Destination Address	4	Destination IP Address

IPv4 Header field requirements for TMoIP are described in Table 3-8.

TABLE 3-8. IPv4 HEADER FIELD REQUIREMENTS

Field	Notes
Version, Header Length	Code to 0x45 to support IP Version 4, header length of 20 bytes
Type of Service	Provide ability for user to modify
Total Length	Calculated value
ID	Can be automatically generated or provide user ability to modify
Flags, Fragment Offset	Can be automatically generated or provide user ability to modify
Time to Live	Can be automatically generated or provide user ability to modify
Protocol Type	Code to 0x11 for UDP
Header Checksum	Calculated value
Source Address	Provide ability for user to modify
Destination Address	Provide ability for user to modify

A key function of the Layer 3 protocol is to provide capability for the transfer of packets between Network Processors located in the Ground Network. Each Network Processor is identified by its IP address. When a packet is prepared for transmission, the IP address of the sending packet is placed into the Source Address Field, and the IP address of the target Network Processor is placed in the Destination Address Field. The intervening network (i.e. the Ground Network in the case of the TMoIP implementation) will enable the delivery of the packet based upon the Destination IP Address contained in the packet.

There are three types of IP addresses:

a. Unicast. Unicast addresses are used for traffic destined for a single host.
b. Broadcast. Broadcast addresses are for traffic destined for all hosts on a given network.
c. Multicast. Multicast addresses are used for traffic destined for a set of hosts that belong to a multicast group.

The TMoIP implementation will support unicast and multicast addresses (Reference j).

The IP address used in multicast operation is called the multicast group address, and has a specific format that includes the multicast group ID. By joining a particular multicast group, a Network Processor can listen to a multicast address and decode the TM stream being sent to that multicast group. There is no restriction for the number of hosts in a group, so an unrestricted number of Network Processors can potentially decode a single TM stream.

Req	The TMoIP implementation shall support unicast and multicast IP addresses

Opt	The TMoIP implementation may provide the capability to assign a separate IP address to each TM stream

3.5.6 Layer 2. Layer 2 of the OSI Model is responsible for packaging raw bits from the physical layer into frames, and for transporting the frames from one host to another. The TMoIP implementation will use the 802.3 (Ethernet) Layer 2 protocol (Reference k). The Ethernet protocol is the dominant Layer 2 protocol in use in IP networks.

The Ethernet overhead consists of header and trailer information that is added to the TMoIP Layer3/Layer 4/Layer 6 Payload, and consists of a total of 22 bytes. The Layer 2 through Layer 6 TMoIP implementation is shown in Figure 3-7. The un-shaded blocks are the overhead added by the Layer 2 protocol.

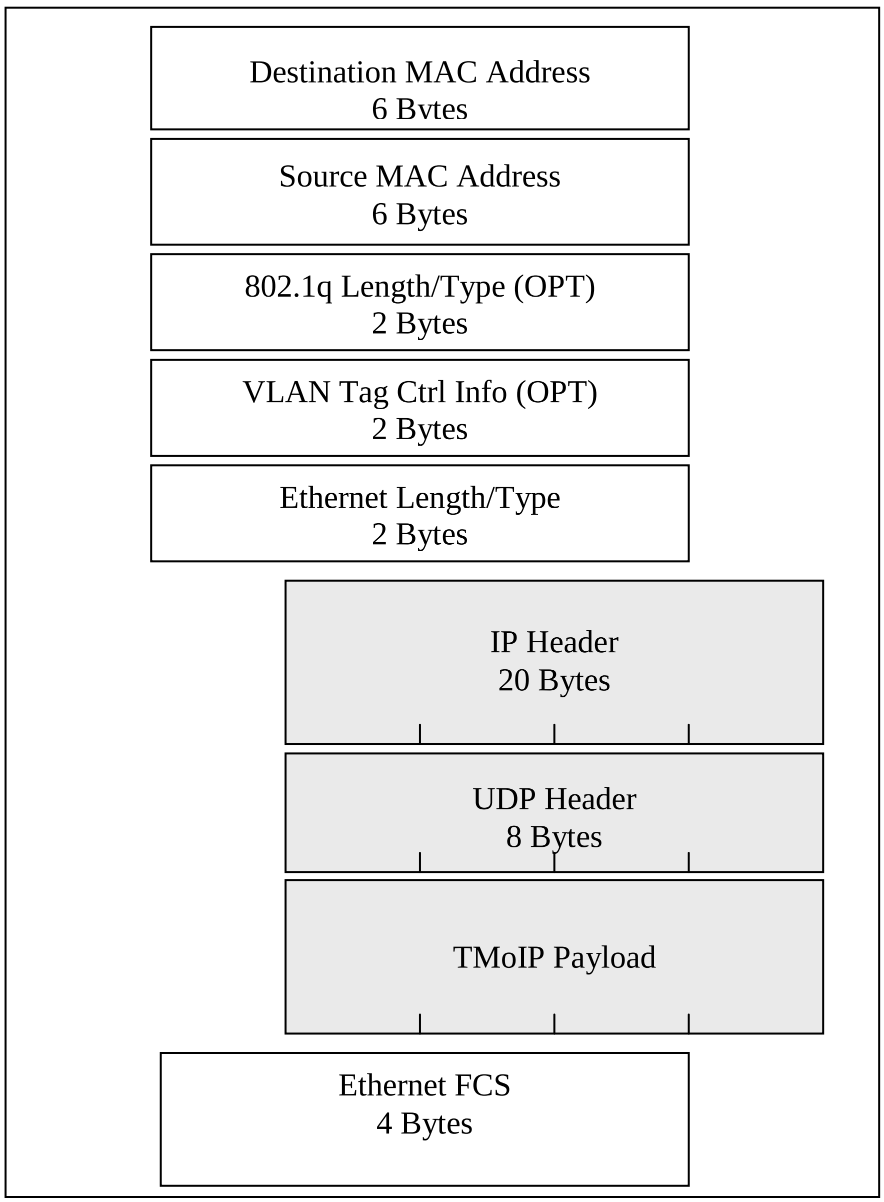


Figure 3-7. TMoIP Layer 2 - Layer 6 implementation.

The Ethernet Overhead Fields are described in Table 3-9.

TABLE 3-9. ETHERNET OVERHEAD FIELDS

<table>
<tr><th>Field</th><th>Len</th><th colspan="2">Description</th></tr>
<tr><td>Ethernet Dest Addr</td><td>6</td><td colspan="2">Destination Address</td></tr>
<tr><td>Ethernet Src Addr</td><td>6</td><td colspan="2">Source Address</td></tr>
<tr><td>802.1Q Length/Type</td><td>2</td><td colspan="2">Indicates that frame contains Virtual Local Area Network (VLAN) tagging</td></tr>
<tr><td rowspan="4">VLAN Tag Ctrl Info</td><td rowspan="4">2</td><td>Bit</td><td>Description</td></tr>
<tr><td>0 - 2</td><td>User Priority Field</td></tr>
<tr><td>3</td><td>Canonical Format Indicator (CFI)</td></tr>
<tr><td>4 - 15</td><td>VLAN Identifier (VID)</td></tr>
<tr><td>Length/Type</td><td>2</td><td colspan="2">Set to 0x0800 (IPv4)</td></tr>
<tr><td>Ethernet FCS</td><td>4</td><td colspan="2">Ethernet Frame Check Sequence, typically generated by Ethernet PHY chip</td></tr>
</table>

The TMoIP requirements for the Ethernet Overhead Fields are described in Table 3-10.

TABLE 3-10. ETHERNET OVERHEAD FIELD REQUIREMENTS

Field	Notes
Ethernet Dest Addr	Provide ability for user to modify
Ethernet Src Addr	Fixed by host hardware
802.1Q Length/Type	Set to 0x8100 to indicate VLAN tag present if used
VLAN Tag Ctrl Info	Provide ability for user to modify
Length/Type	Set to 0x8000 (IPv4)
Ethernet FCS	Calculated value

The 802.1Q Length/Type and Virtual LAN (VLAN) Tag Control Information fields provide support for IEEE 802.1Q functionality. This 4-byte field is frequently referred to as the VLAN tag. The VLAN tag is inserted into the Ethernet frame between the Source MAC Address field and the Length/Type field. The first two bytes consist of the "802.1Q Length/Type" and are set to a value of 0x8100 that indicates the presence of the VLAN tag. The last 2-bytes of the VLAN tag contain the following information:

a. The first 3-bits are a User Priority Field that may be used to assign a priority level to the Ethernet frame.
b. The next 1-bit is a Canonical Format Indicator (CFI) used in Ethernet frames to indicate the presence of a Routing Information Field (RIF).
c. The last 12-bits are the VLAN Identifier (VID) that uniquely identifies the VLAN to which the Ethernet frame belongs.

The IEEE 802.1Q standard allows the transport of separate network streams over a common physical link. In the TMoIP implementation, the VID provides the capability to assign TM streams to a VLAN, and provide switching capability based upon the VLAN.

The user priority field provides mechanism for implementing QoS, as defined by the IEEE 802.1p standard. This 3-bit field supports eight different service classes. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations.

Req	The user shall be capable of assigning the Ethernet Destination Address.

Opt	The TMoIP implementation may provide the capability to assign a separate VLAN ID (VID) to each TM stream.

Opt	The TMoIP implementation may provide the capability to assign the User Priority field (802.1p) to each stream.

3.5.7 Layer 1. Layer 1 of the OSI Model is responsible for connection to the transmission media and defines physical interconnections and the electrical specification of the signals.

The TMoIP implementation will include physical layer mechanisms associated with Ethernet (Reference k). A number of implementations exist for Layer 1 transport of native Ethernet traffic. Table 3-11 below summarizes the required and optional implementations for TMoIP.

Req	The following Layer 1 interfaces shall be supported as shown in Table 3-11.

TABLE 3-11. TMoIP LAYER 1 REQUIREMENTS

Reference	Description	Standard	Support
100BASE-TX	100 Mbit/s over copper/twisted pair	802.3u	Required
100BASE-FX	100 Mbit/s over fiber	802.3u	Optional
10BASE-T	10 Mbit/s over copper/twisted pair	802.3i	Optional
10BASE-F	10 Mbit/s over fiber	802.3j	Optional
1000BASE-X	Gigabit Ethernet over fiber at 1000 Mbit/sec	802.3z	Optional
1000BASE-T	Gigabit Ethernet over twisted pair at 1000 Mbit/sec	802.3ab	Optional

NOTE	To provide user flexibility, it is recommended that support for Gigabit Interface Converter (GBIC)/Small Form-factor Pluggable (SFP) connector interfaces be included in TMoIP equipment that implements fiber optic interfaces.

NOTE	The recommended fiber interface connector types are the SC style (referred to as a subscriber connector, a square connector, or as a standard connector) and the LC style (referred to as a Lucent connector or as a local connector)

3.6 TMoIP Packet Design Summary and Discussion

The TMoIP packet layout is shown in Figure 3-8 below. Each protocol layer adds overhead information to the TMoIP payload, resulting in the final TMoIP packet configuration.

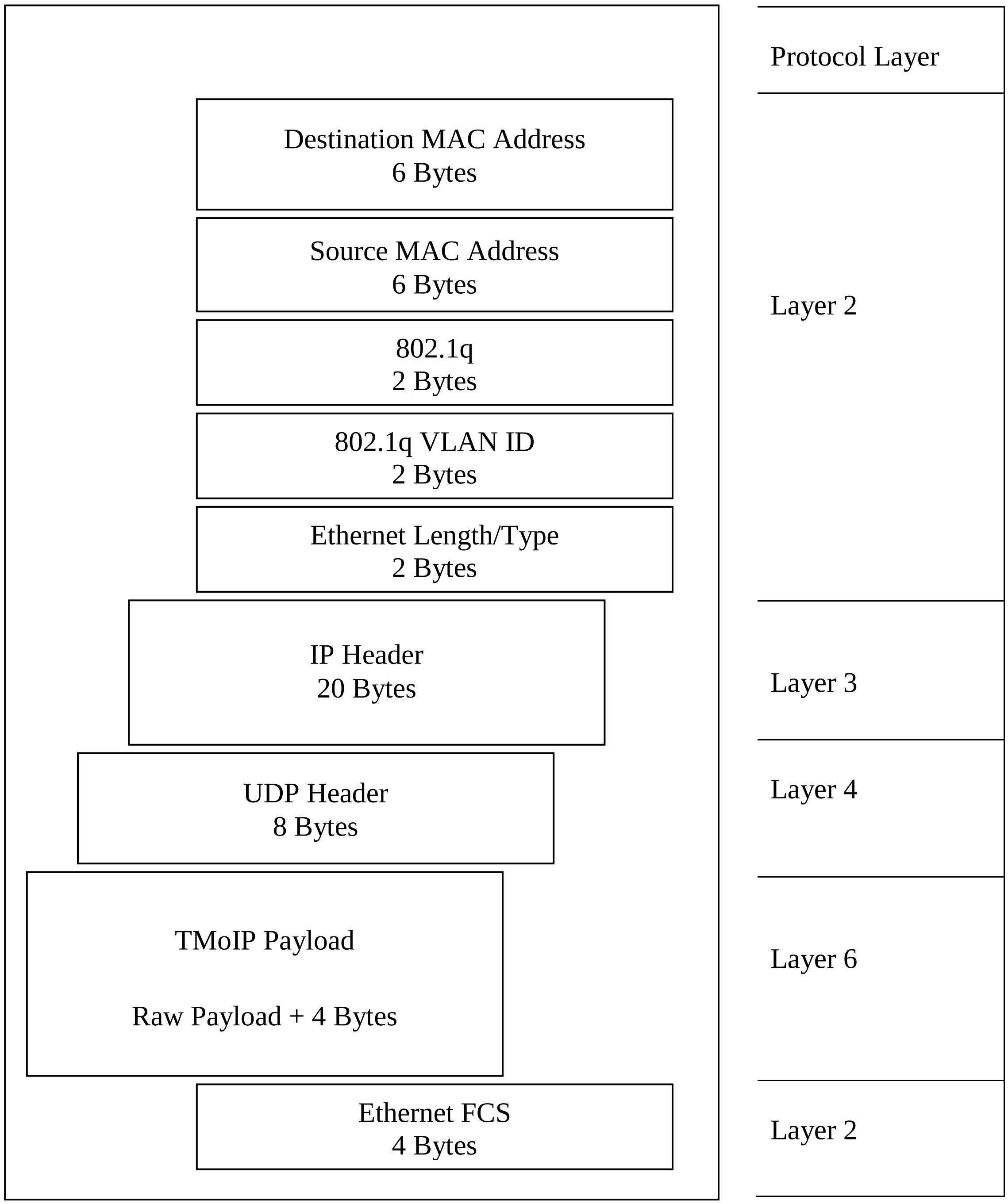


Figure 3-8. TMoIP Packet layout.

The field descriptions for the TMoIP packet are summarized in Table 3-12.

TABLE 3-12. TMoIP PACKET SUMMARY

Field	Description		Length	P/C/F (1)
Ethernet Dest Addr	Identifies station(s) to receive frame		6	P
Ethernet Src Addr	Identifies station that originated frame		6	C
802.1Q Length/Type	Virtual LAN (VLAN) tag length/type		2	F = 0x8100
VLAN Tag Ctrl Info	Bit	Description	2	
	0 - 2	User Priority Field		P
	3	Canonical Format Indicator (CFI)		F = 0
	4 - 15	VLAN Identifier (VID)		P
Length/Type			2	F = 0x0800
IP Header	Byte	Description		
	0	Version + IP header length	1	F = 0x45
20 Bytes Total	1	TOS	1	P
	2 - 3	Total length of IP packet	2	C
	4 - 5	16 bit ID	2	C/F
	6 - 7	Flags + Fragment Offset	2	F
	8	TTL	1	F/P
	9	Protocol (UDP)	1	F = 0x11
	10 - 11	IP Header checksum	2	C
	12 - 15	Source IP address	4	P
	18 - 19	Destination IP address	4	P
UDP Header	Byte	Description		
	0 - 1	Source Port	2	P
8 Bytes Total	2 - 3	Destination Port	2	P
	4 - 5	UDP Length	2	C
	6 - 7	UDP Checksum	2	C
Payload	TMoIP Control Word		4	C
	TM Raw Packet Data		Note (2)	C
Ethernet FCS	Ethernet Frame Check Sequence		4	C

Notes

1. P = Programmable by user, C = Calculated or placed in packet without user intervention, and F = Fixed.
2. Refer to packet discussion, Table 3-13.
3. The following packet constraints have been identified:
    - Ethernet PDU maximum size 1518 bytes.
    - Total packet overhead for Layer 2, Layer 3, and Layer 4 is 46 bytes without 802.1Q tagging support, and 50 bytes with 802.1 tagging support.

A number of possible packet sizes are shown in Table 3-13. The larger packet sizes optimize the required overhead, and the smaller packet sizes optimize delay and tolerance to errors in the network.

TABLE 3-13. SAMPLE PAYLOAD CALCULATIONS

Overhead			TMoIP Payload (1)	Total Payload (2)	Overhead
L2	L3	L4			
22	20	8	68	118	46 %
22	20	8	132	182	30 %
22	20	8	260	310	17 %
22	20	8	516	566	10 %
22	20	8	1028	1078	5 %

Notes

1. TMoIP Payload includes the Raw TM Payload plus 4 bytes for the TMoIP Control Word.
2. The Total Payload includes the TM Payload with the Layer 2, Layer 3, and Layer 4 overhead included. The Layer 2 payload includes support for Virtual LAN (VLAN) overhead.

This page intentionally left blank.

CHAPTER 4

TMOIP MANAGEMENT

The previous chapter defined the requirements for the generation of TMoIP packets for transport over IP networks, whose implementation was supported in the Network Processor functional block. The topics in this chapter consider management level considerations, many of which are implemented in the Ground Network Link and associated end equipment.

4.1 Management Mechanisms

Management capabilities will provide the ability to provision, monitor performance, and manage faults. The management operation can be performed locally or remotely.

Local management supports direct access and provisioning of the Network Processor. Examples of local management include console interfaces, typically implemented using RS-232 or Ethernet connectivity coupled with command line interface (CLI) or menu-driven user interfaces.

Remote management provides the capability to provision and manage the Network Processor when it is located in remote locations in the Ground Network. Examples of remote management configurations in the TCP/IP environment include CLI via the SSH [Secure Shell] application, browser-based applications using HTTPS [Secure Socket Layer], and SNMPv3 [Simple Network Management Protocol].

Inband management provides the capability to manage the Network Processor via the main traffic-bearing interface. Examples of inband management are management via a separate Layer 2 connection such as an IEEE 802.1q VLAN or a separate Layer 3 IP address that provides

Implementation of protocols such as Extensible Markup Language (XML) for integration with higher-level management or data collection domains is left to the discretion of the vendor.

TABLE 4-1. MANAGEMENT MECHANISMS

Req/Opt[1]	Requirement description
Req	TM Terminals shall provide a mechanism to support local management functionality.
Req	TM Terminals shall provide a mechanism to support remote management functionality.
Req	Remote management of TM Terminals shall provide the SSHv2 protocol or higher.
Req	The SSH protocol provided for remote management shall support the TM Terminal CLI .
Opt	The SSH protocol provided for remote management shall provide the mechanism to establish a tunnel for SNMP protocol to pass through.
Opt	Remote management of TM Terminals shall provide the HTTPS protocol.
Req	Remote management of TM Terminals shall provide the SNMP protocol version 3 with backwards compatibility for SNMP version 2c.

[1] Req = Required, Opt = Optional, Note = notes.

A minimum set of alarm, configuration, and statistical parameters is provided. The list of required alarms and configuration parameters to be supported by TM Terminals is provided in Appendix F.

4.2 Quality of Service (QoS)

The TMoIP protocol defined is based upon the IP protocol. The Internet services model (upon which IP is based) of a sender/single receiver is insufficient for real-time data services. In the case of transport of telemetry data, the real-time requirements are particularly important. Therefore QoS mechanisms need to be defined and implemented to support both multicast and real-time (telemetry) service transport.

Diff-serv generically defines a mechanism where traffic is classified into a number of service types, and the flow of traffic is controlled based upon the service type.

The TMoIP QoS scheme is based upon the Diff-serv model for providing quality of service support, and uses the following mechanisms:

a. Traffic classification and prioritization
b. Preferential Queuing of high priority traffic

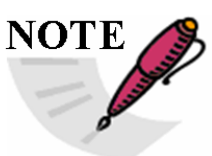
The TMoIP standard will define the means by which the TM packets can be classified. The queuing and preferential treatment of the TM packets is not in the scope of this document, and will be allocated to the Ground Network Link infrastructure (switches, routers) over which the TMoIP packets propagate.

4.2.1 Layer 2 Mechanisms. IEEE 802.1p specification enables Layer 2 switches to prioritize traffic and perform dynamic multicast filtering. The prioritization specification works at the media access control (MAC) framing layer (OSI layer 2) and is therefore called a layer 2 mechanism.

The 802.1p header includes a three-bit field for traffic prioritization, which allows packets to be grouped into various traffic classes. IEEE 802.1p establishes eight levels of priority. The highest priority is seven, which might go to network-critical traffic such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) table updates. Values five and six might be for delay-sensitive applications such as interactive video and voice. Data classes four through one range from controlled-load applications such as streaming multimedia and business-critical traffic – carrying Session Announcement Protocol (SAP) data, for instance – down to “loss eligible” traffic. The zero value is used as a best-effort default, invoked automatically when no other value has been set.

TABLE 4-2. LAYER 2 QoS MECHANISMS

Req/Opt[(1)]	**Requirement description**
Opt	To support Layer 2 QoS mechanisms, the TM Terminal shall provide the ability to modify the VLAN priority bits
[1] Req = Required, Opt = Optional, Notes =notes	



It is recommended that vendors of TMoIP equipment provide shaping of TMoIP streams such that the packet rate at the network ingress has minimum variation.

4.2.2 Layer 3 Mechanisms. QoS support via the Diff-serv model can also be implemented at Layer 3. This supports QoS support for end equipment such as routers that are Layer 3-aware.

TABLE 4-3. LAYER 3 QoS MECHANISMS

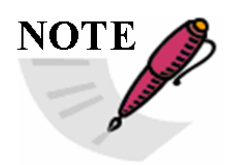
Req/Opt[(1)]	**Requirement description**
Req	To support Layer 3 QoS mechanisms, the TM Terminal shall provide the ability to modify Differentiated Services Codepoint (DSCP) data for each TM flow.
Opt	Support for extended tagging mechanisms, such as Multi-Protocol Label Switching (MPLS) is recommended.
[1] Req = Required, Opt = Optional	

4.3 Network Performance

The characterizations of network performance criteria that impact successful telemetry stream transport over IP networks are described. Quantifying these parameters will be addressed in future versions of the TMoIP implementation standard document.

4.3.1 Packet Delay Variation. As TMoIP packets are generated by a constant rate serial bit stream, the packets will natively be generated at a constant rate. If the packet rate is impacted by variable switching delays as the packet traverses the network, then jitter in the inter-packet delay is introduced. This jitter is more commonly referred to as packet delay variation, and can result in errors in the regenerated stream if the delay between any two packets is increased too much (resulting in underflow in the receive buffer) or too little (resulting in overflow in the receive buffer).

4.3.2 Delay. The causes of delay and its effects were discussed in Section 3.5. In most cases, the largest contribution to delay is incurred in the packet reassembly buffer located at the receiver. One mechanism to mediate the effects of the reassembly buffer delay, and to provide support for a mechanism for performing the temporal alignment of a number of telemetry streams is to provide the ability to adjust the depth of the reassembly buffer is required. Actual implementation details are beyond the scope of this document and will be left to the vendor.

	In any TMoIP solution, it is recommended that considerations for stream alignment be addressed

4.3.3 Network Errors. Potential sources of network errors that can negatively impact TMoIP operation are:

a. Bit errors in network.
b. Dropped packets.
c. Misaligned packets.

Bit errors that occur in the payload will result in bit errors in the regenerated bit stream. Packet level errors can be more problematic, as they impact both the data integrity, and in the case of dropped packets, can produce errors in the recovered clock.

Errors that occur on the packet level can be caused by a number of faults, such as bit errors in the addressing fields that result in non-delivery of the packet, or bit errors in the payload that, upon detection, cause the packet to be dropped.

The effects of a lost packet are twofold: The payload itself is lost, resulting in corruption of the TM data, and when adaptive clock recovery is used, the loss of a packet will cause an error in the recovered clock frequency. To mitigate the effect of a lost packet on the clock recovery mechanism, a "stuff packet" mechanism can be used. A stuff packet is a packet that is inserted into the TMoIP Receiver clock recovery buffer to restore it to the correct level and diminish the effects of a lost packet on the adaptive clock recovery algorithm.

NOTE	It is recommended that the TMoIP adaptive clock recovery algorithm be architected to tolerate dropped packets.

TABLE 4-4. NETWORK PERFORMANCE—DROPPED PACKETS	
Req/Opt[(1)]	**Requirement description**
Req	In order to maintain the adaptive clock recovery mechanism, the capability to insert stuff packets at the RX Telemetry Terminal when a packet loss is detected shall be supported
Req	The user shall have the ability to enable or disable the packet-stuffing feature on a per stream basis.
Req	The stuff packet shall be composed of a series of identical bytes. The data pattern of the stuff byte shall be user defined.
[1] Req = Required, Opt = Optional, Note = notes	

4.4 IPV4 to IPV6 Migration

The current version of the TMoIP specification defines operation in IPv4 [IPv4] network infrastructures. As IPv6 networks [IPv6] become more prevalent, the need to generate native IPV6 traffic will become necessary. Currently, end-to-end networks that support IPV6 traffic are not common enough to warrant the requirement for native IPV6 packet construction for the current revision of this document.

TABLE 4-5. IPV4/IPV6 REQUIREMENTS	
Req/Opt[(1)]	**Requirement description**
Req	The TM Terminal shall generate packets compliant to IPv4
Req	The TM Terminal shall generate packets compliant to IPv6
[1] Req = Required, Opt = Optional, Note = note	

NOTE	It is recommended that vendors of TMoIP equipment design the architecture of the packetizing engine using programmable logic that has the ability to provide dual-stack operation.

NOTE	Transport of TMoIP traffic over IPV6 equipment is recommended to be supported via tunneling techniques. The tunneling functionality is reserved for external routers in the Ground Network.

NOTE	This version of the TMoIP standard intends for IPv6 addressing features only to be supported. Support for additional features of IPv6 is left to the description of the manufacturer. IPv6 advanced features will be further developed in a future version of this standard.

4.5 Multicast Support

An important feature of the IP protocol is the ability to natively support multicast traffic. This section will identify considerations when multicasting TM streams.

IP Multicast supports communications from one transmitter to multiple receivers over an IP network. Support for a large number of receivers is inherent, as the identity of the receiver and the number of receivers is not required. Multicast is bandwidth efficient, because the transmitter has to send the packet only once. The packets are replicated by the downstream nodes as required to support delivery to all receivers.

Multicast packets use special types of IP addresses that identifies to the network that the packet contains multicast traffic. These IP addresses are referred to as Multicast group addresses. At the network ingress, the Network TX Stream will be constructed with the multicast group address as the destination address. If a node wants to receive traffic from a particular multicast group, it must inform the network. In this fashion, the receiver "joins" the multicast group. Once the receiver has joined a particular multicast group, the network equipment in the path forwards the packets for that multicast group to the receiver. If no receivers have joined a multicast group, the network equipment will not forward these packets. In this fashion, multicast traffic only consumes network bandwidth when a receiver requests the traffic. The protocol used by receivers to join a multicast group is called or the Internet Group Management Protocol (IGMP).

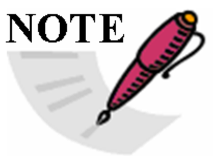
Multicast addresses are identified by the pattern "1110" in the first four bits, which corresponds to a first octet of 224 to 239. The full range of multicast addresses is from 224.0.0.0 to 239.255.255.255.

An additional set of protocols Session Announcement Protocol (SAP), and Session Description Protocol (SDP), allows multicast senders to communicate the characteristics of their multicast streams to potential receivers. The receivers monitor the SAP packets to identify potential streams that they may want to decode. The SAP listening applications can listen to the well-known SAP multicast address and construct a guide of all advertised multicast sessions. SAP uses SDP as the format of the session descriptions.

For TMoIP vendors that enable multicast support, the following recommendations are made:

TABLE 4-6. MULTICAST PACKETS

Req/Opt[1]	**Requirement description**
Req	TM Terminals that transmit to the Ground Network shall support the generation of multicast packets with a user-programmable Multicast Group Address
Req	TM Terminals that receive from the Ground Network shall support the IGMP version 2 or higher protocols to join and leave multicast groups.
[1] Req = Required, Opt = Optional, Note = notes	

	It is recommended that TMoIP transmitters support generation of SAP/SDP messaging to advertise their content

This page intentionally left blank.

APPENDIX A

REFERENCES

a. [TM_1] RCC Document 106-07 Part I - Telemetry Standards.

b. [TM_2] RCC Document 106-07 Part II - Telemetry Networks.

c. [Pseudo Wire_1] Request for Comments (RFC) 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture.

d. [Pseudo Wire_2] RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3).

e. [Pseudo Wire_3] RFC 4553 Structure Agnostic Time Division Multiplexing (TDM) over Packet (SAToP).

f. [RTP] RFC 1889 RTP: A Transport Protocol for Real-Time Applications.

g. [UDP] RFC 768 User Datagram Protocol (UDP).

h. [TCP] RFC 761 Transmission Control Protocol.

i. [IPv4] RFC 791 (STD0005) Internet Protocol (IP).

j. [Multicast] RFC 1112 Host Extensions for IP Multicasting.

k. [Ethernet] IEEE 802.3 Ethernet.

l. [MPOA] RFC 2684 Multi-Protocol Encapsulation over ATM Adaptation Layer 5.

m. [AAL1] ITU-T Recommendation I.363.1 (08/96) B-ISDN ATM Adaptation Layer (AAL) specification: Type 1.

n. [AAL5] ITU-T Recommendation I.363.5 (11/00) B-ISDN ATM Adaptation Layer (AAL) specification: Type 5.

o. [CES] ATM forum specification atm-vtoa-0078 (CES 2.0) Circuit Emulation Service Interoperability Specification Ver. 2.0.

p. [FIPS] Federal Information Processing Standards (FIPS) PUB 140-2 Security Requirements for Cryptographic Modules.

q. [IGMP] RFC 3376 Internet Group Management Protocol Version 3.

r. [IPPM] RFC 2330 Framework for IP Performance Metrics.

s. [IPv6] RFC 2460 Internet Protocol, Version 6 Specification.

t. [L2TPv3] Draft-ietf-l2tpext-l2tp-base-01.txt Layer Two Tunneling Protocol (L2TP).

u. [MIB] RFC 1212 Concise Management Information Base (MIB) Definitions.

v. [MPLS] RFC 3031 Multi-Protocol Label Switching Architecture.

w. [NTP] RFC 1305 Network Time Protocol (NTP) (Version 3) Specification, Implementation and Analysis.

x. [SAP] RFC 2974 Session Announcement Protocol.

y. [SDP] RFC 2327 SDP: Session Description Protocol.

z. [SNMP] RFC 1157 A Simple Network Management Protocol (SNMP).

aa. [TDMoIP] IETF draft-anavi-tdmoip-03, TDM over IP.

APPENDIX B

COMMON ABBREVIATIONS AND DEFINITIONS

AAL	ATM Adaptation Layer
AIS	Airborne Instrumentation System
ATM	Asynchronous Transfer Mode: A protocol that formats data traffic into fixed length packets for transmission through the network.
CDH	Communications Distribution Hub
CE	Customer Edge: The term used in Pseudo Wire protocol descriptions, and refers to a device where one end of a service originates and/or terminates. The CE is not aware that it is using an emulated service rather than a native service.
CES	Circuit Emulation Service: enables support of TDM stream transport over ATM networks.
CFI	Canonical Format Indicator
CLI	Command Line Interface: provides the mechanism for communicating with a local or remote system via a series of typed commands.
COTS	Commercial off the Shelf
datagram	A formatted block of information carried by a network. The term is generally reserved for packets that are not transported reliably.
demultiplex demultiplexer demux	The inverse operation of multiplexing, where the combined signal stream is split into its separate source signals.
Diff-serv	Differentiated Services: mechanism used to provide Quality of Service (QoS) on IP networks. Diff-serve uses traffic classification and prioritization to enable preferential delivery of time-sensitive traffic such as TM streams.
DS3	Digital Signal 3: a PDH signal that provides transport of digital bitstreams. The signaling rate of the DS3 signal is 44.736 Mbits/sec
DSCP	Differentiated Services Codepoint
DVMRP	Distance Vector Multicast Routing Protocol
FCS	Frame Check Sequence
FIPS	Federal Information Processing Standards
FTS	Flight Termination System

GBIC	Gigabit Interface Converter
GND NW LINK	Ground Network Link
HTTP	Hypertext Transfer Protocol: a communication protocol for information transfer on the World Wide Web.
IANA	Internet Assigned Numbers Authority
IEEE	International Institute of Electrical and Electronics Engineers
IEEE 802.1Q	A set of standards maintained by the IEEE that define a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (trunking). IEEE 802.1Q also defines the meaning of a virtual LAN (VLAN).
IEEE 802.3 802.3 x	A set of standards maintained by the IEEE that define the physical layer and Media Access Control (MAC) layer for wired Ethernet networks.
IGMP	Internet Group Management Protocol: IGNP is used to manage the membership of multicast groups. This protocol allows network nodes and their locally connected routers to receive multicast streams from the source node.
informative	Information provided for completeness. Not required for standard compliance.
interoperability	The capability to communicate or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.
IP	Internet Protocol: IP provides global, unique address functionality between end nodes.
IPPM	IP Performance Metrics
IPv4	Internet Protocol version 4, fourth and most widely deployed version of the Internet Protocol.
IPv6	Internet Protocol version 6: the designated successor to IPv4
jitter	Unwanted variation of the interval between successive pulses in a digital signal. Phase variations with frequency content above 10 Hz are considered jitter.
L	Local Defect Alarm (field name reference)
L2TP	Layer Two Tunneling Protocol (L2TP).
LAN	Local Area Network
LC	Lucent connector; local connector
LEN	LEN (field name reference to “length”)

M	Local Defect Alarm Modifier (field name reference)
MIB	Management Information Base: a database used by SNMP to manage nodes in and IP network
MPLS	Multi-Protocol Label Switching
MPOA	Multi-Protocol Encapsulation over ATM
MTU	Maximum Transmission Unit
multicast	The delivery of traffic to a group of nodes simultaneously.
multiplex multiplexer mux	A device or the activity that combines a number of signals together to transport on a single channel.
node	A point of connection into a network.
node synchronization	The ability to time synchronize two or more nodes to a common time base.
NRZ	Non-Return-to-Zero
NRZ-L	Non-Return-to-Zero Level
NRZ-M	Non-Return-to-Zero Mark
NRZ-S	Non-Return-to-Zero Space
NTP	Network Time Protocol
NW	Network
NW PROC	Network Processor
OC12	Optical Carrier 12: a SONET signal that provides transport of digital bitstreams. The signaling rate of the OC3 signal is 622.08 Mbits/sec.
OC3	Optical Carrier 3: a SONET signal that provides transport of digital bitstreams. The signaling rate of the OC3 signal is 155.52 Mbits/sec.
OEM	Original Equipment Manufacturer
open systems	A well-defined open set of interfaces and protocols that facilitates the development of new features by third party vendors.
Opt.	Optional: requirement, may or may not be implemented.
OSI	Open Standard Interconnect; Open Systems Interconnection
OSI Model	A layered, abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnection initiative. It is also called the OSI Seven Layers Model.

OSPF	Open Shortest Path First: a protocol used by IP routers to determine most efficient paths for traffic. It is generally acknowledged that OSPF is superior to and the successor to Routing Information Protocol (RIP).
packet	A formatted block of information carried by a network. In the TMoIP standard, the term packet will be used to define the fundamental unit of exchange for TM streams over IP networks.
PC	Payload Convergence: the term used in Pseudo Wire protocol descriptions, and refers to the operation of adapting the serial bit stream to a packetized stream for subsequent transport over a packet switched network.
PDH	Plesiochronous Digital Hierarchy: a telecommunications technology used to transport digital bitstreams across copper, fiber, and microwave networks
PE	Provider Edge: term used in Pseudo Wire protocol descriptions, and refers to a device that provides PWE3 to a CE.
PIM	Protocol-Independent Multicast: a family of multicast routing protocols, enables the generation of routing information to provide efficient distribution of multicast streams over an IP network.
port	Network access point for data entry or exit.
protocol	A procedure for adding order to the exchange of data. A specific set of rules, procedures, or conventions relating to format and timing of data transmission between two devices.
Pseudo Wire	Provides emulation of a native service over a packet switched network.
PW	PseudoWire
QoS	Quality of Service: a set of mechanisms that are used to guarantee a level of performance to a data stream across a network. The QoS functions by providing different priority levels to traffic based upon user requirements.
R	Remote Defect Alarm (field name reference)
Req	Required element, must be included to be compliant with TMoIP standard.
RES	Reserved (field name reference)
RES	Reserved (field name reference)
RF	Radio Frequency
RFC	Request For Comments
RIF	Routing Information Field

RIP	Routing Information Protocol: a protocol used by routers in IP networks to exchange connection information and allow routers to adapt to changes in network connections to provide delivery of traffic.
RTP	Real-time Transport Protocol: defines a standardized packet format for delivering audio and video over the Internet.
SAP	Session Announcement Protocol: a protocol for broadcasting multicast session information.
SAToP	Structure Agnostic Time Division Multiplexing (TDM) over Packet
SC	subscriber connector; square connector; standard connector
SDP	Session Description Protocol: a format for describing streaming media parameters.
SEQ NUMBER	Sequence Number (field name reference)
SFP	Small Form-factor Pluggable
SIG PROC	Signal Processor
SNMP	Simple Network Management Protocol: used by network management systems to monitor nodes for status and alarm conditions.
SONET	Synchronous Optical Networking: a method of transporting digital streams over optical networks. The SONET methodology was developed as a replacement technology for PDH networks.
SSH	Secure Shell
STP	Spanning Tree Protocol: a protocol that functions to prevent loops in IP networks, by disabling loops that occur and can negatively impact network performance.
TCP	Transmission Control Protocol: TCP guarantees reliable and in-order delivery of data from sender to receiver over packet switched networks.
TDM	Time Division Multiplexing: a method of simultaneously transporting a number of sub-channels in one communication channel, by physically taking turns on the channel.
TDMoIP	TDM over IP
telemetry	Refers to technology that enables measurement and transport of information of a remote system to an operator.
TELNET	Terminal Emulation program for TCP/IP networks. Protocol definition RFC 854.

time correlation	The ability to correlate two or more data samples with respect to the time they were sampled.
time synchronization	The ability to synchronize two or more sources.
TM	Telemetry
TM TERM	TM Terminal
TMoIP	Telemetry Transmission over IP Protocol: defines a set of mechanisms to enable transport of telemetry streams across IP networks.
UDP	User Datagram Protocol: enables networked computers to send short messages to one another. Note: UDP does not provide the reliability and ordering guarantees that TCP does.
UHF	Ultra High Frequency
unicast	The delivery of traffic to a single node.
VHF	Very High Frequency
VID	VLAN Identifier
VLAN	Virtual LAN: a mechanism that enables the creation of multiple logical networks within a single physical network.
wander	Refers to random variations of the significant instants of a digital signal from their ideal positions. Phase variations with frequency content below 10 Hz are referred to as wander.
XML	Extensible Markup Language: a markup language that allows information to be shared between different computer systems, especially on the Internet

APPENDIX C

RECOMMENDATIONS FOR TM TERMINAL LAYER 1

This appendix provides recommendations and guidelines for the Layer 1 (Physical Layer) implementation of the TM Terminal (see Table C-1).

TABLE C-1. RECOMMENDATIONS AND GUIDELINES FOR THE LAYER 1 (PHYSICAL LAYER) IMPLEMENTATION OF THE TM TERMINAL

Category	Recommendation/Guideline
a. Physical	
Req	BNC-type connectors with an impedance of 50 ohms
Opt	Support of RS530 physical interface
b. Electrical	
Req	Single-ended TTL electrical
Opt	Balanced electrical interface
Req	Support rate adaptive mechanism for signaling rate reconstruction
Opt	Provide for migration to signaling rates to 100 Mbit/sec
c. Encoding	
Req	Encoding shall comply with encoding requirements specified in IRIG 106 Chapter 4 for Non-Return-to-Zero Level (NRZ-L) serial streams
Opt	Streams can optionally support the remaining IRIG 106 Chapter 4 encoding schemes, including: • Viterbi • Non-Return-to-Zero Mark (NRZ-M) • Non-Return-to-Zero Space (NRZ-S) • Randomized • Biphase-L
Note: Req = Required Opt = Optional	

This page intentionally left blank.

APPENDIX D

CONSIDERATIONS FOR LEGACY ASYNCHRONOUS TRANSFER MODE (ATM) INTERWORKING

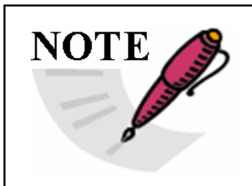
This appendix describes Telemetry over Internet Protocol (TMoIP) implementation considerations for occasions when the packetized TMoIP stream is subsequently transported over an ATM network. Many ranges still use Asynchronous Transfer Mode (ATM) technology in the backbone. Considering this fact when constructing the TMoIP stream can offer transport efficiencies, particularly during the process of converting from IP packets to ATM cells.

The IP over ATM encapsulation mechanism (Reference l, RFC 2684 Multi-Protocol Encapsulation over ATM (MPOA) initially produces an IP stream from the TM stream source. This mechanism encapsulates the stream using the Request for Comments (RFC) 2684 encapsulation scheme for transporting IP packets over ATM networks. This process generates ATM cells that carry the IP packets.

Several possible packet sizes are shown in Table D-1 for optimal RFC 2684 encapsulation. The optimal encapsulation provides the most efficient encapsulation of the TMoIP packet into the RFC 2684 format. If the optimal encapsulation is used, then all of the cells in the ATM are completely filled and no bandwidth is wasted because there are no partially filled cells.

TABLE D-1. REQUEST FOR COMMENTS (RFC) 2684 OPTIMAL PAYLOADS

Number of ATM Cells	Total Bytes 53/cell	ATM Payload 48/cell	TMoIP Payload	TMoIP Raw Payload	Percent Overhead
20	1060	960	942	888	16
15	785	720	702	648	17
10	530	480	462	408	23
6	318	288	270	153	52
3	159	144	126	72	55



Supporting the packet sizes in Table C-1 provides the most efficient payloads for transport over ATM networks.

This page intentionally left blank.

APPENDIX E

SUMMARY OF REQUIREMENTS

This appendix summarizes the required and optional parameters of the Telemetry over Internet Protocol (TMoIP) implementation. For example, a TMoIP field description summary for the packet is in Table E-1; all notational items, as in footnote 1 of Table E-1, are included for reference purposes.

The following provides links to the requirement topics covered in Appendix E.

TABLE E-1. TMoIP PACKET SUMMARY				
Field	**Description**		**Length**	**P/C/F** [1]
Ethernet Dest Addr	Identifies station(s) to receive frame		6	P
Ethernet Src Addr	Identifies station that originated frame		6	C
802.1Q Length/Type	Virtual LAN (VLAN) tag length/type		2	F = 0x8100
VLAN Tag Ctrl Info	Bit	Description	2	
	0 - 2	User Priority Field		P
	3	Canonical Format Indicator (CFI)		F = 0
	4 - 15	VLAN Identifier (VID)		P
Length/Type			2	F = 0x0800
IP Header	Byte	Description		
	0	Version + IP header length	1	F = 0x45
20 Bytes Total	1	TOS	1	P
	2 - 3	Total length of IP packet	2	C
	4 - 5	16 bit ID	2	C/F
	6 - 7	Flags + Fragment Offset	2	F
	8	TTL	1	F/P
	9	Protocol (UDP)	1	F = 0x11
	10 - 11	IP Header checksum	2	C
	12 - 15	Source IP address	4	P
	18 - 19	Destination IP address	4	P
UDP Header	Byte	Description		
	0 - 1	Source Port	2	P
8 Bytes Total	2 - 3	Destination Port	2	P
	4 - 5	UDP Length	2	C
	6 - 7	UDP Checksum	2	C
Payload	TMoIP Control Word		4	C
	TM Raw Packet Data		Var	C
Ethernet FCS	Ethernet Frame Check Sequence		4	C

[1] P = Programmable by user.
C = Calculated or placed in packet without user intervention.
F = Fixed.
Var = Variable.

TABLE E-2. HIGH LEVEL REQUIREMENTS
(Reference Paragraph 3.2)

Required/ Optional	Comment
Req	Accurately and reliably transport and regenerate the source TM data and timing across the network.
Req	Support an Encode/Decode latency of less than 100 milliseconds for the TM input stream to the TM output stream for the following TM rates: 100 Kb/s < TM Stream Rate < 35 Mbps
Req	Enable the use of Quality of Service (QoS) mechanisms that are available in Commercial Off the Shelf (COTS) network equipment.
Req	The transport mechanism for uplink streams must support message validation and re-transmission.
Req	Support local and remote management mechanisms to provision and monitor the TMoIP equipment.

TABLE E-3. TMoIP CONTROL WORD FORMAT
(Reference Paragraph **3.5.2b**)

Required/ Optional	Comment
Req	The TMoIP raw packet size shall be user configurable
Opt	The TMoIP raw payload size may be auto-configurable, based on user priorities (e.g. stream/delay characteristics)
Req	The minimum TMoIP raw packet size = 1 byte

Notes:

a. To limit the effects of Ethernet fragmentation, the final Layer 2/3/4/6 packet size should be less than the maximum Ethernet Maximum Transmission Unit (MTU).
b. Padding may be required to meet the minimum Ethernet MTU size

TABLE E-4. PACKET SIZE
(Reference Paragraph 3.5.2c)

Note:

Support for packet designs that simplify inter-working with alternate protocols may be included. One example is to provide the capability to generate packets that can be efficiently packed into Multi-Protocol-Over-ATM (RFC 2684) cells.

TABLE E-5. CLOCK RECOVERY (Reference Paragraph 3.5.2D(1))				
Required/ Optional	**Comment**			
Req	Adaptive clock recovery support is required for TM clock regeneration			
Opt	RTP support is optional			
Req	The clock recovery algorithm must display the following performance characteristics:			
	Spec	**Min**	**Max**	**Notes**
				Per IRIG 106 Chapter 4
	Wander			Per IRIG 106 Chapter 4
	Acquisition Time		N/A	TM stream rate $\leq$ 64 Kbps
	Acquisition Time		2 sec	TM stream rate > 64 Kbps Acquire to $\pm$ 500 ppm from stream resynchronization

TABLE E-6. TIMED DELIVERY (Reference Paragraph 3.5.2d(2))	
Required/ Optional	**Comment**
Opt	Support for timed delivery is optional at this time, but equipment vendors are urged to consider implementation of this feature in their equipment.

TABLE E-7. USER DIAGRAM PROTOCOL (UDP) (Reference Paragraph 3.5.4a)	
Required/ Optional	**Comment**
Req	UDP protocol support shall be included in the TMoIP implementation
Opt	The TMoIP implementation may provide the capability to assign a separate UDP port to each TM stream
Opt	The TMoIP implementation may provide the capability to assign a separate UDP port to management streams
Req	The TMoIP implementation shall support the use of UDP ports 49152 through 65535

TABLE E-8. TRANSMISSION CONTROL PROTOCOL (TCP) (Reference Paragraph 3.5.4b)
Note: TCP implementations may be considered in future versions of the TMoIP standard.

TABLE E-9. LAYER 3
(Reference Paragraph 3.5.5)

Required/ Optional	Comment
Req	The TMoIP implementation shall support unicast and multicast IP addresses
Opt	The TMoIP implementation may provide the capability to assign a separate IP address to each TM stream

TABLE E-10. LAYER 2
(Reference Paragraph 3.5.6)

Required/ Optional	Comment
Req	The user shall be capable of assigning the Ethernet Destination Address
Opt	The TMoIP implementation may provide the capability to assign a separate VLAN ID to each TM stream
Opt	The TMoIP implementation may provide the capability to assign the User Priority field (802.1p) to each stream

TABLE E-11. LAYER 1
(Reference Paragraph 3.5.7)

Required/ Optional	Comment			
Req	The following Layer 1 interfaces shall be supported as shown below:			
	Reference	**Description**	**Standard**	**Support**
	100BASE-TX	100 Mbit/s over copper/twisted pair	802.3u	Required
	100BASE-FX	100 Mbit/s over fiber	802.3u	Optional
	10BASE-T	10 Mbit/s over copper/twisted pair	802.3i	Optional
	10BASE-F	10 Mbit/s over fiber	802.3j	Optional
	1000BASE-X	Gigabit Ethernet over fiber at 1000 Mbit/sec	802.3z	Optional
	1000BASE-T	Gigabit Ethernet over twisted pair at 1000 Mbit/sec	802.3ab	Optional

Notes:
a. To provide user flexibility, it is recommended that support for GBIC/SFP connector interfaces be included in TMoIP equipment that implements fiber optic interfaces.
b. The recommended fiber interface connector types are "SC" or "LC" styles.

TABLE E-12. MANAGEMENT MECHANISMS (Reference Paragraph 4.1)	
Required/ Optional	**Comment**
Req	TM Terminals shall provide a mechanism to support local management functionality.
Req	TM Terminals shall provide a mechanism to support remote management functionality.

TABLE E-13. LAYER 2 QoS MECHANISMS (Reference Paragraph 4.2.1)	
Required/ Optional	**Comment**
Opt	To support Layer 2 Quality of Service (QoS) mechanisms, provide the ability to modify the VLAN priority bits
Note	It is recommended that vendors of TMoIP equipment provide shaping of TMoIP streams such that the packet rate at the network ingress has minimum variability.
Note	For support of legacy layer 2 QoS schemes, the vendor can provide a mapping of QoS mechanisms between IP and ATM networks. By mapping different VLANs to ATM connections with configured traffic classes, it is possible to bridge ATM and IP networks while maintaining the Layer 2 QoS.

TABLE E-14. LAYER 3 QoS MECHANISMS (Reference Paragraph 4.2.2)	
Required/ Optional	**Comment**
Req	To support Layer 3 Quality of Service (QoS) mechanisms, provide the ability to modify Differentiated Services Codepoint (DSCP) data for each TM flow.
Opt	Support for extended tagging mechanisms, such as MPLS is recommended

TABLE E-15. STREAM ALIGNMENT (Reference Paragraph 4.3.2)	
Required/ Optional	**Comment**
Note	In any TMoIP solution, considerations for stream alignment must be addressed

TABLE E-16. ADAPTIVE CLOCK RECOVERY (Reference Paragraph 4.3.3)	
Required/ Optional	**Comment**
Note	It is recommended that the TMoIP adaptive clock recovery algorithm be architected to tolerate dropped packets.

TABLE E-17. NETWORK PERFORMANCE—DROPPED PACKETS (Reference Paragraph 4.3.3)	
Required/ Optional	**Comment**
Req	In order to maintain the adaptive clock recovery mechanism, the capability to insert stuff packets at the RX Telemetry Terminal when a packet loss is detected shall be supported
Req	The user shall have the ability to enable or disable the packet stuffing feature on a per stream basis.
Req	The stuff packet shall be composed of a series of identical bytes. The data pattern of the stuff byte shall be user defined.

TABLE E-18. IPV4 TO IPV6 MIGRATION (Reference Paragraph 4.4)	
Required/ Optional	**Comment**
Req	The TMoIP implementation shall generate packets compliant to IPV4
Note	It is recommended that vendors of TMoIP equipment design the architecture of the packetizing engine using programmable logic that has the ability to migrate to IPV6 support via system firmware upgrades.
Note	Transport of TMoIP traffic over IPV6 equipment is recommended to be supported via tunneling techniques. The tunneling functionality is reserved for external routers in the Ground Network.

TABLE E-19. MULTICAST PACKETS (Reference Paragraph 4.5)	
Required/ Optional	**Comment**
Req	It is recommended TMoIP transmitters support generation of multicast packets with a user-programmable Multicast Group Address
Req	It is recommended TMoIP receivers support IGMP message protocol to join multicast groups
Note	It is recommended that TMoIP transmitters support generation of SAP/SDP messaging to advertise their content

This page intentionally left blank.

APPENDIX F

SUMMARY OF MANAGED OBJECTS

This appendix summarizes the required and optional parameters of the Telemetry Transmission over Internet Protocol (TMoIP) implementation. These managed objects are relevant to TMoIP transport function of the equipment that implements TMoIP. Additional managed objects may be implemented, but their definition is not in the scope of this document.

The following requirement topics are covered in this appendix.

TABLE F-1. ALARMS

Type	Description	Notes
Physical	TM Input Fault (Note 1)	Per TMoIP flow
Physical	Ethernet link failure	Per Ethernet port
Protocol	Local Defect Alarm (Note 2)	Per TMoIP flow
Protocol	Remote Defect Alarm (Note 3)	Per TMoIP flow
Protocol	Ingress FIFO Overrun	Per TMoIP flow
Protocol	Egress FIFO Overrun	Per TMoIP flow
Protocol	Egress FIFO Underrun	Per TMoIP flow

Notes

1. TM Input Fault is defined as telemetry stream that is out of compliance with IRIG 106.
2. Local Defect Alarm is indicated by “L” Bit in TMoIP Control Word (Ref Table 3-3).
2. Remote Defect Alarm is indicated by “R” Bit in TMoIP Control Word (Ref Table 3-3).

TABLE F-2. CONFIGURATION PARAMETERS

Type	Description	Notes
Rx Parameters	Rx Destination IP Address	Accept IP Port
	Rx Destination UDP Port	Accept UDP Port
	Rx Destination MAC Address	Accept MAC Address
	Rx 802.1p Priority	
	Rx 802.1p VLAN ID	
	Rx DSCP	
	Rx IGMP	Enable IGMP Support to respond to IGMP Query packets
	Filter Enable/Select	Accept IP Port, UDP Port, MAC Address
Tx Parameters	Tx Destination IP Address	Target IP Port
	Tx Destination MAC Address	Target MAC Address
	Tx Destination UDP Port	Target UDP Port
	Tx Source IP Port	
	Tx Source MAC Address	Read-Only
	Tx Source UDP Port	
	Tx 802.1p Tag	Enable/Disable (Opt)
	Tx 802.1p Priority	
	Tx 802.1p VLAN ID	
	Tx DSCP	
	Tx ARP	Enable/Disable
	Tx Data Length	
	Packet Size	
Port	TM Port Configuration Parameters	Vendor defined port configuration parameters
Statistics	Clear Stats Counters	

TABLE F-3. TM STATISTICS

Type	Description	Notes
TM Frame, RX	Reassembled TMoIP Packets	Number of raw TMoIP packets received and reassembled
	Sequence Errors	Detected in TMoIP Control Word
	FIFO Overruns	
	Dropped Reassembled TMoIP Packets	Number of TMoIP packets dropped
TM Frame, TX	Assembled TMoIP Packets	Number of raw TMoIP packets assembled for transmission
	FIFO Overruns	
	FIFO Underruns	

TABLE F-4. ETHERNET STATISTICS		
Type	**Description**	**Notes**
Rx Frame Counts	Received Frames	Total all received Ethernet frames
	Good Frames	
	Forwarded Frames	Forwarded to upper layer
	Forwarded Octets	Forwarded to upper layer
Rx Discard Frames	Total Frame Discards	Total all discards
	Rx Buffer Discards	Discards due to buffer overrun
	Rx Error Discards	Total discards due to errors
	Frame Collision	
	Pause Frames	Indicates flow control events
Tx Frame Counts	Transmitted Frames	Total all transmitted Ethernet frames
	Good Frames	
	Frames Sent	
	Octets Sent	
	Pause Frames	
	Queue Overflow	
Tx Discard Frames	Total Frame Discards	Total all transmit frame discards
	Tx Buffer Discards	Discards due to buffer overrun
	Tx Error Discards	
	Late Collision Discards	
	Carrier loss Discards	
	Retransmit Limit Discards	

APPENDIX G

APPLICATION NOTES

This appendix provides additional application information that, while not in the scope of the TMoIP requirements, is intended to provide information to the user to enable the deployment of a network infrastructure that supports the TMoIP implementation.

1.1 Security

In the scope of the TMoIP protocol, security applies to two functions:

a. Secure transmission of TM streams.
b. Secure transmission of management information.

Given that TM streams are source-encrypted, the aspect of security is reserved for the Provider Edge, and is outside of the scope of the TMoIP protocol. However, some recommendations will be made to promote network compatibility, and to frame the discussion for future implementations.

For applications outside the scope of Type 1 encryption, use of encryption compliant to FIPS-140-2 Level 2 [FIPS] is recommended. FIPS-140 is a set of cryptographic standards issued by the NIST for used by departments and agencies of the US Government. Support for FIPS is becoming available in Provider Edge equipment.

NOTE	It is recommended that the TMoIP implementation and connected infrastructure provide support or migration to FIPS-140 encryption.

For applications that require Type 1 encryption it is recommended that the Ground Network Link equipment allow for IP encapsulation through the use a tunneling protocol such as GRE. This becomes especially important where the traffic is Multicast and not entirely Unicast, as Type 1 cryptos prohibit the transport of Multicast streams.

NOTE	For installations that require the use of Type 1 encryption, it is recommended that the Ground Network Link equipment support an IP tunneling protocol to enable tunneling of multicast traffic through the cryptos.

To enable the secure transmission of management information, Version 3 of the Simple Network Management Protocol (SNMP) protocol provides support for encryption, authentication, and access control of management packets.

NOTE	It is recommended that TMoIP implementations that support SNMP management provide immediate support or a migration path to SNMP version 3.

1.2 Reliability and Redundancy

As the IP protocol suite was intended for the best effort delivery of traffic, reliability was not a prime consideration when the protocol was originally conceived. However, there exist mechanisms in the IP protocol that can be used to provide increased reliability. This section provides an overview of techniques that can be used to enhance the reliability of the Ground Network Link.

The Spanning Tree protocol can be used as a mechanism to provide redundant operation. The Spanning Tree Protocol (STP) is a Layer 2 mechanism that ensures the existence of a loop free network topology for any LAN. Spanning Tree functions to eliminate broadcast storms in a mesh network by disabling links that incur loops in the network.

Spanning Tree can be used to provide network redundancy in the following fashion:

a. Design the TMoIP link to intentionally have two paths between endpoints, introducing a loop in the network
b. Enable the operation of Spanning Tree in the Ground Network Link equipment.
c. The Spanning Tree algorithm will disable one of the paths at all times. If at some point the active path is disabled, the alternate path will become the active path.

This scheme requires the following:

d. All equipment in the Ground Network Link must be STP-enabled
e. All equipment must have the same version of STP

This scheme lends itself to the current generation of end equipment that support enhanced fail-over switching to provide a self-healing network topology.

In addition to providing redundant service, the reliability of the TMoIP network implementation can be improved by providing protection against link oversubscription. IP is a protocol that does not require end stations that are about to transmit to communicate with each other (or establish a connection) prior to the transmission of traffic. One drawback of this scheme is that if too many end stations generate traffic simultaneously, the payload capacity of the network may be exceeded. In the case of the transmission of multiple high bandwidth real time TM streams, this is a realistic concern.

1.3 Multicast Routing Considerations

In addition to the requirements to enable the transport of multicast TM traffic, the need exists for routing support of multicast traffic. This function is supported via a set of multicast routing protocols. These protocols function to construct multicast distribution trees so that data can flow from senders of multicast traffic to all receivers that have joined the group. This function is of particular importance in complex IP networks, where the source traffic must span a number of routers to reach its destination node.

The implementation of multicast routing is reserved for the Provider Edge, and is outside of the scope of the TMoIP protocol. However, some application information is presented below to assist the network designer.

1.3.1 <u>Current Multicast Routing Protocols</u>. The following three multicast routing protocols currently used to a significant extent are:

a. Protocol Independent Multicast Sparse Mode (PIM-SM).
b. Protocol Independent Multicast Dense Mode (PIM-DM).
c. Distance Vector Multicast Routing Protocol (DVMRP).

1.3.2 <u>Selection Considerations</u>. In the selection of the multicast routing protocol, the following considerations should be addressed:

a. <u>Base Requirement</u>. In simple, linear network configurations multicast routing is not required and only adds to network complexity.
b. <u>Opt-in vs. Opt-out routing</u>. Multicast routing protocols are differentiated into two basic schemes. In an opt-in implementation, multicast traffic is not transmitted until the routing tree has been constructed. This scheme is bandwidth-efficient, especially in networks where a relative few number of nodes will receive the multicast traffic. In an opt-out implementation, the multicast traffic is initially broadcast to the network, and routers disable or "prune" multicast traffic forwarding if the downstream nodes are not members of that particular multicast group. This scheme is very efficient when the network is densely populated with nodes that will receive the multicast traffic.
c. <u>Signaling</u>. Multicast routing requires signaling traffic to be exchanged between routers to support the construction of the multicast routing trees. The potential effects of this traffic on the timely delivery of real-time TM streams must be considered by the network planner.

END OF RCC DOCUMENT

****** NOTHING FOLLOWS ******